Translations proofread by EDPB Members.

This language version has not yet been proofread.

Retningslinjer 5/2022 for anvendelse af ansigtsgenkendelsesteknologi på retshåndhævelsesområdet

Version 2.0

Vedtaget den 26. april 2023

Versionsoversigt

Version 1.0	12. maj 2022	Vedtagelse af retningslinjerne til offentlig høring
Version 2.0	26. april 2023	Vedtagelse af retningslinjerne efter offentlig høring

Indholdsfortegnelse

Resumé 5

1 Indledning 8

2 Teknologi 9

2.1 Én biometrisk teknologi, to særskilte funktioner 9

2.2 En bred vifte af formål og anvendelser 11

2.3 Pålidelighed, nøjagtighed og risici for de registrerede 13

3 Gældende retlige rammer 14

3.1 Generel retlig ramme – EU's charter om grundlæggende rettigheder og den europæiske menneskerettighedskonvention (EMRK) 15

3.1.1 Chartrets anvendelighed 15

3.1.2 Indgreb i de rettigheder, der er fastsat i chartret 15

3.1.3 Begrundelser for indgreb 16

3.2 Specifik juridisk ramme – direktivet om retshåndhævelse 21

3.2.1 Behandling af særlige kategorier af data til retshåndhævelsesformål 21

3.2.2 Automatiske individuelle afgørelser, herunder profilering 23

3.2.3 Kategorier af registrerede 24

3.2.4 Den registreredes rettigheder 25

3.2.5 Andre juridiske krav og sikkerhedsforanstaltninger 28

4 Konklusion 31

5 Bilag 32

Bilag I – Skabelon til beskrivelse af scenarier 33

Bilag II – Praktisk vejledning for retshåndhævende myndigheder i håndtering af projekter med ansigtsgenkendelsesteknologi 35

1. ROLLER OG ANSVARSOMRÅDER 35

2. OPRETTELSE/INDEN INDKØB AF SYSTEMET FOR ANSIGTSGENKENDELSESTEKNOLOGI 37

3. UNDER INDKØB OG INDEN IVÆRKSÆTTELSE AF ANSIGTSGENKENDELSESTEKNOLOGIEN 39

4. ANBEFALINGER EFTER IVÆRKSÆTTELSE AF ANSIGTSGENKENDELSESTEKNOLOGIEN 40

Bilag III – PRAKTISKE EKSEMPLER 42

1 Scenarie 1 42

1.1. Beskrivelse 42

1.2. Gældende retlige rammer 43

1.3. Nødvendighed og proportionalitet – forbrydelsens formål/alvorlighed 43

1.4. Konklusion 44

2 Scenarie 2 44

2.1. Beskrivelse 44
2.2. Gældende retlige rammer 45
2.3. Nødvendighed og proportionalitet – forbrydelsens formål/alvor/antal personer, der ikke er involveret, men som er berørt af behandlingen 45
2.4. Konklusion 46
3 Scenarie 3 46
3.1. Beskrivelse 46
3.2. Gældende retlige rammer 48
3.3. Nødvendighed og proportionalitet 48
3.4. Konklusion 49
4 Scenarie 4 49
4.1. Beskrivelse 49
4.2. Gældende retlige rammer 50
4.3. Nødvendighed og proportionalitet 50
4.4. Konklusion 50
5 Scenarie 5 51
5.1. Beskrivelse 51
5.2. Gældende retlige rammer 52
5.3. Nødvendighed og proportionalitet 52
5.4. Konklusion 55
6 Scenarie 6 55
6.1. Beskrivelse 55
6.2. Gældende retlige rammer 55
6.3. Nødvendighed og proportionalitet 56
6.4. Konklusion 56

RESUMÉ

Stadig flere retshåndhævende myndigheder anvender eller har til hensigt at anvende ansigtsgenkendelsesteknologi. Denne teknologi kan bruges til at **autentificere** eller til at **identificere** en person og kan anvendes på videoer (f.eks. overvågningskameraer) eller fotografier. Den kan anvendes i forskellige situationer, herunder til at søge efter personer på politiets overvågningslister eller til at overvåge en persons bevægelser i det offentlige rum.

Ansigtsgenkendelsesteknologi er baseret på behandling af **biometriske data** og omfatter derfor behandling af særlige kategorier af personoplysninger. Ofte anvender ansigtsgenkendelsesteknologi komponenter af **kunstig intelligens** eller maskinlæring. Selv om dette muliggør databehandling i stor skala, medfører det også en risiko for forskelsbehandling og falske resultater. Ansigtsgenkendelsesteknologi kan både anvendes i kontrollerede 1:1-situationer, men også på store menneskemængder og ved vigtige transportknudepunkter.

Ansigtsgenkendelsesteknologi bør betragtes som et **følsomt værktøj for retshåndhævende myndigheder.** Retshåndhævende myndigheder er udøvende myndigheder og har suveræne beføjelser. Ansigtsgenkendelsesteknologi kan gribe ind i grundlæggende rettigheder – også ud over retten til beskyttelse af personoplysninger – og påvirke vores sociale og demokratiske politiske stabilitet.

Med hensyn til beskyttelse af personoplysninger i forbindelse med retshåndhævelse skal **kravene i retshåndhævelsesdirektivet** opfyldes. Der er fastsat en bestemt ramme for anvendelse af ansigtsgenkendelsesteknologi i retshåndhævelsesdirektivet, navnlig artikel 3, stk. 13 (udtrykket "biometriske data"), i artikel 4 (principper for behandling af personoplysninger), artikel 8 (lovlig behandling), artikel 10 (behandling af særlige kategorier af personoplysninger) og artikel 11 (automatiske individuelle afgørelser).

Flere andre grundlæggende rettigheder kan også blive berørt af anvendelsen af ansigtsgenkendelsesteknologi. Derfor er **EU's charter om grundlæggende rettigheder** ("chartret") afgørende for fortolkningen af retshåndhævelsesdirektivet, navnlig retten til beskyttelse af personoplysninger i chartrets artikel 8, men også retten til respekt for privatliv, som fremgår af chartrets artikel 7.

Lovgivningsmæssige foranstaltninger, der tjener som retsgrundlag for behandling af personoplysninger, berører direkte de rettigheder, der er sikret ved chartrets artikel 7 og 8. Behandling af biometriske data udgør under alle omstændigheder et alvorligt indgreb i sig selv. Dette afhænger ikke af resultatet, f.eks. en positiv matchning. Enhver begrænsning i udøvelsen af grundlæggende rettigheder og frihedsrettigheder skal være fastsat ved lov og respektere essensen i disse rettigheder og frihedsrettigheder.

Retsgrundlaget skal være **tilstrækkeligt klart** i sin ordlyd til at give borgerne en passende indikation af de betingelser og omstændigheder, hvorunder myndighederne har beføjelse til at anvende enhver form for indsamling af data og hemmelig overvågning. En simpel gennemførelse i national ret af den generelle bestemmelse i retshåndhævelsesdirektivets artikel 10 ville mangle præcision og forudsigelighed.

Før en national lovgiver skaber et nyt retsgrundlag for enhver form for behandling af biometriske data ved hjælp af ansigtsgenkendelse, bør den kompetente databeskyttelsestilsynsmyndighed **høres**.

Lovgivningsmæssige foranstaltninger skal være **passende** for at nå de legitime mål, der forfølges af den pågældende lovgivning. Et **mål af almen interesse** – uanset hvor grundlæggende det måtte være – kan ikke i sig selv begrunde en begrænsning af en grundlæggende rettighed. En lovgivningsmæssig foranstaltning bør **differentiere** og være målrettet mod de personer, der i lyset af dens mål er omfattet af den, f.eks. bekæmpelse af specifik alvorlig kriminalitet. Hvis foranstaltningen dækker alle personer på en generel måde uden en sådan differentiering, begrænsning eller undtagelse, forstærker den indgrebet. Det udgør ligeledes en intensivering af indgrebet, hvis databehandlingen omfatter en betydelig del af befolkningen.

Oplysningerne skal behandles på en måde, der sikrer anvendeligheden og effektiviteten af EU's databeskyttelsesregler og -principper. Baseret på hver enkelt situation skal alle mulige konsekvenser for andre grundlæggende rettigheder også klarlægges og overvejes i forbindelse med **vurderingen af nødvendighed og proportionalitet**. Hvis dataene behandles systematisk uden de registreredes viden, kan det føre til, at der opstår en **generel følelse af konstant overvågning**. Dette kan have afskrækkende virkninger hvad angår nogle eller alle af de berørte grundlæggende rettigheder, herunder den menneskelige værdighed i henhold til chartrets artikel 1, retten til at tænke frit og til samvittigheds- og religionsfrihed i henhold til chartrets artikel 10, ytringsfrihed i henhold til chartrets artikel 11 samt forsamlings- og foreningsfrihed i henhold til chartrets artikel 12.

Behandling af særlige kategorier af data såsom biometriske data kan kun betragtes som "**strengt nødvendigt**" (artikel 10 i retshåndhævelsesdirektivet), hvis indgrebet i beskyttelsen af personoplysninger og dets begrænsninger er begrænset til, hvad der er absolut nødvendigt, dvs. uundværligt, og udelukker enhver behandling af generel eller systematisk karakter.

Det faktum, at et fotografi **tydeligvis er offentliggjort** (artikel 10 i retshåndhævelsesdirektivet) af den registrerede, medfører ikke, at de relaterede biometriske data, som kan hentes fra fotografiet med specifikke tekniske midler, anses for tydeligvis offentliggjorte. Standardindstillinger for en tjeneste, f.eks. at skabeloner gøres offentligt tilgængelige, eller mangel på valgmuligheder, f.eks. at skabeloner gøres offentligt tilgængelige, uden at brugeren kan ændre denne indstilling, bør ikke på nogen måde fortolkes som data, der tydeligvis er offentliggjorte.

Artikel 11 i retshåndhævelsesdirektivet etablerer en ramme for **automatiske individuelle afgørelser**. Anvendelsen af ansigtsgenkendelsesteknologi indebærer anvendelse af særlige kategorier af oplysninger og kan føre til profilering, afhængigt af hvordan og med hvilket formål den anvendes. I overensstemmelse med EU-retten og artikel 11, stk. 3, i retshåndhævelsesdirektivet er profilering, der fører til forskelsbehandling af fysiske personer på grundlag af særlige kategorier af personoplysninger, under alle omstændigheder forbudt.

Artikel 6 i retshåndhævelsesdirektivet omhandler nødvendigheden af at **sondre mellem forskellige kategorier af registrerede**. For de registrerede, for hvilke der ikke foreligger beviser, der kan tyde på, at deres adfærd kan have en forbindelse, selv indirekte eller fjern, med det legitime formål i henhold til retshåndhævelsesdirektivet, er der højst sandsynligt ingen begrundelse for et indgreb.

Princippet om dataminimering (artikel 4, stk.1, litra e), i retshåndhævelsesdirektivet) indebærer også, at ethvert videomateriale, der ikke er relevant for formålet med behandlingen, altid bør fjernes eller anonymiseres (f.eks. ved sløring uden mulighed for senere at gendanne dataene) inden anvendelse.

Den dataansvarlige skal nøje overveje, hvordan (hvis overhovedet) kravene til den **registreredes rettigheder** kan opfyldes, inden ansigtsgenkendelsesteknologi tages i brug, da den ofte indebærer behandling af særlige kategorier af personoplysninger uden nogen åbenbar interaktion med den registrerede.

En effektiv udøvelse af den registreredes rettigheder afhænger af, at den dataansvarlige opfylder sine **oplysningsforpligtelser** (artikel 13 i retshåndhævelsesdirektivet). Ved vurderingen af, om der foreligger "et særligt tilfælde" i henhold til retshåndhævelsesdirektivets artikel 13, stk. 2, skal der tages hensyn til flere faktorer, herunder om personoplysninger indsamles uden den registreredes vidende, hvor kendskab hertil ville være den eneste måde, hvorpå den registrerede effektivt kunne udøve sine rettigheder. Hvis beslutningstagningen udelukkende udføres på grundlag af ansigtsgenkendelsesteknologi, skal den registrerede informeres om elementerne i den automatiske afgørelse.

For så vidt angår **anmodninger om indsigt**, bør dette, når biometriske data lagres og forbindes med en identitet, også ved hjælp af alfanumeriske data, i overensstemmelse med princippet om dataminimering give den kompetente myndighed mulighed for at efterkomme en anmodning om indsigt baseret på en søgning med disse alfanumeriske data og uden at indlede yderligere behandling af andres biometriske data (f.eks. ved at søge med ansigtsgenkendelsesteknologi i en database).

Risiciene for de registrerede er særligt alvorlige, hvis urigtige oplysninger opbevares i en politidatabase og/eller deles med andre enheder. Den dataansvarlige skal **berigtige** opbevarede data og systemer til behandling af ansigtsgenkendelsesteknologi i overensstemmelse hermed (se også betragtning 47 i retshåndhævelsesdirektivet).

Retten til **begrænsning** bliver især vigtig, når det drejer sig om brug af ansigtsgenkendelsesteknologi (baseret på en eller flere algoritmer og derved aldrig med et endeligt resultat) i situationer, hvor der indsamles store mængder data, og hvor nøjagtigheden og kvaliteten af identifikationen kan variere.

En **konsekvensanalyse vedrørende databeskyttelse** før anvendelsen af ansigtsgenkendelsesteknologi er et obligatorisk krav, jf. artikel 27 i retshåndhævelsesdirektivet. Databeskyttelsesrådet anbefaler som en tillids- og gennemsigtighedsforbedrende foranstaltning at offentliggøre resultaterne af sådanne analyser eller som minimum de vigtigste resultater og konklusioner af konsekvensanalysen.

De fleste tilfælde af ibrugtagning og anvendelse af ansigtsgenkendelsesteknologi indebærer en iboende høj risiko for registreredes rettigheder og frihedsrettigheder. Derfor bør myndigheder, der implementerer ansigtsgenkendelsesteknologi, **høre** den kompetente tilsynsmyndighed forud for iværksættelsen af systemet.

I betragtning af de biometriske datas entydige karakter bør myndigheder, der iværksætter og/eller bruger ansigtsgenkendelsesteknologi, være særlig opmærksom på **behandlingssikkerheden** i overensstemmelse med artikel 29 i retshåndhævelsesdirektivet. De retshåndhævende myndigheder skal især sikre, at systemet overholder de relevante standarder og iværksætter foranstaltninger til beskyttelse af biometriske skabeloner. Det er vigtigt, at databeskyttelsesprincipper og -garantier integreres i teknologien inden påbegyndelsen af behandlingen af personoplysninger. Selv når en retshåndhævende myndighed har til hensigt at anvende ansigtsgenkendelsesteknologi fra eksterne leverandører, skal den derfor, f.eks. gennem udbudsproceduren, sikre, at der kun iværksættes ansigtsgenkendelsesteknologi, der bygger på principperne om **databeskyttelse gennem design og databeskyttelse gennem standardindstillinger**.

Logning (se artikel 25 i retshåndhævelsesdirektivet) er en vigtig sikkerhedsforanstaltning til kontrol af lovligheden af behandlingen, både internt (dvs. egenkontrol af den berørte dataansvarlige/databehandler) og af eksterne tilsynsmyndigheder. I forbindelse med ansigtsgenkendelsessystemer anbefales også logning for ændringer af referencedatabasen og for identifikations- eller verifikationsforsøg, herunder bruger-, resultat- og konfidensscore. Logning er imidlertid kun ét væsentligt element i det overordnede **ansvarlighedsprincip** (jf. artikel 4, stk. 4, i

retshåndhævelsesdirektivet). Den dataansvarlige skal kunne påvise, at behandlingen er i overensstemmelse med de grundlæggende databeskyttelsesprincipper i artikel 4, stk. 1-3, i retshåndhævelsesdirektivet.

EDPB minder om sin og EDPS' fælles **opfordring til et forbud** mod visse former for behandling i forbindelse med 1) biometrisk fjernidentifikation af personer i offentligt tilgængelige rum, 2) AI-støttede ansigtsgenkendelsessystemer, der kategoriserer personer baseret på deres biometri i klynger i henhold til etnicitet, køn, såvel som politisk eller seksuel orientering eller andre former for forskelsbehandling, 3) brug af ansigtsgenkendelse eller lignende teknologier til at udlede følelser hos en fysisk person og 4) behandling af personoplysninger i en retshåndhævende sammenhæng gennem anvendelse af en database bestående af personoplysninger, der er indsamlet i stor skala og på en vilkårlig måde, f.eks. ved "scraping" af fotografier og ansigtsbilleder, der er tilgængelige online.

En central garanti for de grundlæggende rettigheder, der står på spil, er **effektiv overvågning** fra de kompetente databeskyttelsestilsynsmyndigheders side. Medlemsstaterne skal derfor sikre, at tilsynsmyndighedernes ressourcer er hensigtsmæssige og tilstrækkelige til, at de kan opfylde deres mandat.

Disse **retningslinjer henvender sig til** lovgivere på EU-plan og på nationalt niveau og til retshåndhævende myndigheder og deres medarbejdere, når de iværksætter og bruger systemer med ansigtsgenkendelsesteknologi. Enkeltpersoner er omfattet i det omfang, de er generelt interesserede eller berørt som registrerede, især hvad angår registreredes rettigheder.

Retningslinjerne har til formål at informere om en række egenskaber ved ansigtsgenkendelsesteknologi og de gældende retlige rammer for retshåndhævelsen (navnlig retshåndhævelsesdirektivet).

- Derudover udgør de et **værktøj til støtte for en indledende klassificering af følsomheden i en given use case** (bilag I).
- De indeholder også **praktisk vejledning for retshåndhævende myndigheder, der ønsker at anskaffe og anvende et system med ansigtsgenkendelsesteknologi** (bilag II).
- Retningslinjerne beskriver også flere typiske **use cases og opregner en række relevante overvejelser**, især med hensyn til nødvendigheds- og proportionalitetstesten (bilag III).

1 INDLEDNING

1. Ansigtsgenkendelsesteknologi kan bruges til automatisk at genkende personer ud fra deres ansigt. Teknologien er ofte baseret på kunstig intelligens som f.eks. maskinlæringsteknologier. Anvendelser af ansigtsgenkendelsesteknologi bliver testet og brugt inden for stadig flere områder lige fra individuel brug til private organisationer og offentlig administration. De retshåndhævende myndigheder forventer en række fordele ved anvendelsen af ansigtsgenkendelsesteknologi. Teknologien stiller løsninger på relativt nye udfordringer i udsigt som f.eks. efterforskninger, der involverer store mængder indsamlet bevismateriale, men også på kendte problemer, især med hensyn til manglende personale til observations- og eftersøgningsopgaver.

2. En stor del af den øgede interesse for ansigtsgenkendelsesteknologi skyldes dens effektivitet og skalerbarhed. Med det følger der en række ulemper, der er forbundet med teknologien og dens anvendelse – også i stor skala. Selv om tusindvis af personlige datasæt kan analyseres med et enkelt tryk på en knap, kan selv små effekter af algoritmisk forskelsbehandling eller fejlidentifikation medføre

ulemper for et stort antal individer, der påvirkes alvorligt i deres adfærd og daglige liv. Selve omfanget af behandlingen af personoplysninger, og navnlig biometriske data, er endnu et centralt element i ansigtsgenkendelsesteknologien, hvor behandlingen af personoplysninger udgør et indgreb i den grundlæggende ret til beskyttelse af personoplysninger som fastlagt i artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder (chartret).

3. De retshåndhævende myndigheders anvendelse af ansigtsgenkendelsesteknologi vil få – og har i et vist omfang allerede fået – betydelige konsekvenser for enkeltpersoner og for grupper af mennesker, herunder mindretal. Disse konsekvenser vil også have betydelige virkninger for den måde, vi lever sammen på, og for vores sociale og demokratiske politiske stabilitet, hvor vi lægger vægt på pluralisme og politisk opposition. Retten til beskyttelse af personoplysninger er ofte en afgørende forudsætning for at sikre andre grundlæggende rettigheder. Anvendelsen af ansigtsgenkendelsesteknologi kan i høj grad gribe ind i grundlæggende rettigheder, der går videre end blot retten til beskyttelse af personoplysninger.

4. Databeskyttelsesrådet finder det derfor vigtigt at bidrage til den igangværende integration af ansigtsgenkendelsesteknologi på den del af retshåndhævelsesområdet, der er omfattet af retshåndhævelsesdirektivet[1] og de nationale love, der gennemfører det, ved at fremlægge disse retningslinjer. Retningslinjerne har til formål at tilvejebringe relevante oplysninger til lovgivere på EU-plan og nationalt plan samt til de retshåndhævende myndigheder og deres medarbejdere, når de iværksætter og anvender systemer med ansigtsgenkendelsesteknologi. Retningslinjernes anvendelsesområde er begrænset til ansigtsgenkendelsesteknologi. Når retshåndhævende myndigheder behandler personoplysninger baseret på biometriske data på andre måder, navnlig hvis de behandles på afstand, kan det imidlertid indebære lignende eller yderligere risici for enkeltpersoner, grupper og samfundet. Under hensyntagen til de relevante omstændigheder kan nogle aspekter af disse retningslinjer således også fungere som en nyttig kilde i sådanne sager. Endelig kan enkeltpersoner, der er generelt interesserede eller berørt som registrerede, også finde vigtige oplysninger, især hvad angår registreredes rettigheder.

5. Retningslinjerne består af et hoveddokument og tre bilag. Det foreliggende hoveddokument præsenterer teknologien og de gældende juridiske rammer. Som en hjælp til at identificere nogle af de vigtigste aspekter, når alvoren af indgrebet i de grundlæggende rettigheder på et bestemt anvendelsesområde skal klassificeres, kan skabelonen i bilag I anvendes. Retshåndhævende myndigheder, der ønsker at anskaffe og anvende et system med ansigtsgenkendelsesteknologi, kan finde praktisk vejledning i bilag II. Alt efter ansigtsgenkendelsesteknologiens anvendelsesområde kan forskellige overvejelser være relevante. Et sæt hypotetiske scenarier og relevante overvejelser kan findes i bilag III.

2 TEKNOLOGI

2.1 Én biometrisk teknologi, to særskilte funktioner

6. Ansigtsgenkendelse er en probabilistisk teknologi, der automatisk kan genkende personer baseret på deres ansigt og dermed autentificere eller identificere dem.

[1] Europa-Parlamentets og Rådets direktiv (EU) nr. 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA.

7. Ansigtsgenkendelsesteknologi falder ind under den bredere kategori biometrisk teknologi. Biometri omfatter alle automatiserede processer, der anvendes til at genkende en person ved at kvantificere fysiske, fysiologiske eller adfærdsmæssige karakteristika (fingeraftryk, irisstruktur, stemme, gangart, blodkarmønstre osv.). Disse karakteristika er defineret som "biometriske data", fordi de muliggør eller bekræfter en entydig identifikation af den pågældende person.

8. Det gælder for menneskers ansigter eller, mere specifikt for den tekniske behandling af ansigterne ved hjælp af ansigtsgenkendelsesudstyr, at med et billede af et ansigt (et fotografi eller en video), som kaldes en biometrisk "prøve", er det muligt at udtrække en digital repræsentation af forskellige karakteristika for dette ansigt (dette kaldes en "skabelon").

9. En biometrisk skabelon er en digital repræsentation af de entydige træk fra en biometrisk prøve, og den kan gemmes i en biometrisk database[2]. Denne skabelon formodes at være entydig og specifik for hver person, og den kan i princippet ikke ændres med tiden[3]. I genkendelsesfasen sammenligner enheden denne skabelon med andre skabeloner, der tidligere er produceret eller beregnet direkte fra biometriske prøver i form af ansigter fra billeder, fotografier eller videoer. "Ansigtsgenkendelse" er derfor en proces i to trin: indsamling af ansigtsbilledet og dets omdannelse til en skabelon efterfulgt af genkendelse af dette ansigt ved at sammenligne den tilsvarende skabelon med en eller flere andre skabeloner.

10. Ligesom andre biometriske processer kan ansigtsgenkendelse opfylde to forskellige funktioner:

    - **autentifikation** af en person, der har til formål at verificere, at en person er den, han eller hun udgiver sig for at være. I så fald sammenligner systemet en på forhånd registreret biometrisk skabelon eller prøve (f.eks. lagret på et smartcard eller biometrisk pas) med et enkelt ansigt, f.eks. på en person, der vil passere et kontrolpunkt, for at kontrollere, om der er tale om én og samme person. Denne funktion består derfor af sammenligning mellem to skabeloner. Dette kaldes også 1:1-**verifikation**

    - **identifikation** af en person med det formål at finde en person blandt en gruppe af personer inden for et specifikt område, på et billede eller i en database. I dette tilfælde skal systemet behandle alle indsamlede ansigter for at generere en biometrisk skabelon og derefter kontrollere, om den matcher med en person, som systemet kender. Denne funktionalitet er således afhængig af at sammenligne en skabelon med en database bestående af skabeloner eller prøver (baseline). Dette kaldes også 1:mange-identifikation. Denne proces kan f.eks. forbinde personnavnsdata (efternavn, fornavn) med et ansigt, hvis sammenligningen udføres med en database over fotografier, der er knyttet til efternavne og fornavne. Der kan også være tale om at følge en person gennem en menneskemængde uden nødvendigvis at knytte en forbindelse til personens civile identitet.

11. I begge tilfælde er de anvendte ansigtsgenkendelsesteknikker baseret på et estimeret match mellem skabeloner: den, der sammenlignes, og en eller flere baselines. Fra dette synspunkt er processen probabilistisk: Sammenligningen bestemmer en højere eller lavere sandsynlighed for, at personen faktisk er den person, der skal autentificeres eller identificeres, og hvis denne sandsynlighed overstiger en vis tærskel i systemet, defineret af brugeren eller udvikleren af systemet, vil systemet antage, at der er et match.

[2] Retningslinjer for ansigtsgenkendelse, det rådgivende udvalg for konvention nr. 108 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger, Europarådet, juni 2021.
[3] Dette kan afhænge af typen af biometri og den registreredes alder.

12. Selv om de to funktioner – autentifikation og identifikation – er forskellige, vedrører de begge behandling af biometriske data relateret til en identificeret eller identificerbar fysisk person og udgør derfor en behandling af personoplysninger, og mere specifikt en behandling af særlige kategorier af personoplysninger.

13. Ansigtsgenkendelse er en del af et bredere spektrum af teknikker til behandling af videobilleder. Nogle videokameraer kan filme mennesker inden for et bestemt område, navnlig deres ansigter, men de kan ikke anvendes som sådan til automatisk genkendelse af enkeltpersoner. Det samme gælder for simpel fotografering: Et kamera er ikke et ansigtsgenkendelsessystem, da fotografier af mennesker skal behandles på en bestemt måde for at kunne udtrække biometriske data.

14. Den blotte detektering af ansigter ved hjælp af såkaldte "intelligente" kameraer udgør heller ikke nødvendigvis et ansigtsgenkendelsessystem. Selv om digitale teknikker til at opdage unormal adfærd eller voldelige begivenheder eller til at genkende ansigtsfølelser eller endda silhuetter også rejser vigtige spørgsmål med hensyn til etik og effektivitet, kan de ikke nødvendigvis betragtes som biometriske systemer, der behandler særlige kategorier af personoplysninger, forudsat at de ikke har til formål entydigt at identificere en person, og at den pågældende behandling af personoplysninger ikke omfatter andre særlige kategorier af personoplysninger. Disse eksempler er ikke helt uden forbindelse til ansigtsgenkendelse, men er stadig omfattet af reglerne om beskyttelse af personoplysninger[4]. Hertil kommer, at denne type detektionssystem kan bruges sammen med andre systemer, der har til formål at identificere en person, og dermed kan det betragtes som en ansigtsgenkendelsesteknologi.

15. I modsætning til systemer til videooptagelse og -behandling, der f.eks. kræver installation af fysiske enheder, er ansigtsgenkendelse en softwarefunktion, der kan implementeres i eksisterende systemer (kameraer, billeddatabaser osv.). En sådan funktionalitet kan derfor forbindes eller kobles til en lang række systemer og desuden kombineres med andre funktionaliteter. Denne integration i en allerede eksisterende infrastruktur kræver særlig opmærksomhed, da den indebærer iboende risici på grund af det forhold, at teknologien til ansigtsgenkendelse ikke påkalder sig opmærksomhed og let kan skjules[5].

2.2 En bred vifte af formål og anvendelser

16. Ud over anvendelsesområdet for disse retningslinjer og for retshåndhævelsesdirektivet kan ansigtsgenkendelse anvendes til en lang række andre formål, både til kommerciel brug og til at løse problemer vedrørende offentlig sikkerhed eller retshåndhævelse. Denne teknologi kan anvendes i mange forskellige sammenhænge: i et personligt forhold mellem en bruger og en tjeneste (adgang til en applikation), for at få adgang til et bestemt sted (fysisk filtrering) eller uden nogen særlig begrænsning i det offentlige rum (live ansigtsgenkendelse). Ansigtsgenkendelse kan anvendes på alle slags registrerede: en tjenestes kunde, en ansat, en simpel tilskuer, en eftersøgt person eller en person, der er involveret i juridiske eller administrative procedurer osv. Nogle anvendelser er allerede almindelige og udbredte, mens andre på nuværende tidspunkt er på det eksperimentelle eller spekulative stadie. Selv om disse retningslinjer ikke gælder for alle sådanne anvendelser og applikationer, minder Databeskyttelsesrådet om, at de kun må iværksættes, hvis de er i overensstemmelse med de gældende retlige rammer og navnlig med databeskyttelsesforordningen

[4] Artikel 10 i retshåndhævelsesdirektivet (eller artikel 9 i GDPR) finder imidlertid anvendelse på systemer, der bruges til at kategorisere personer på grundlag af deres biometri i klynger efter etnicitet samt politisk eller seksuel orientering eller andre særlige kategorier af personoplysninger.
[5] For eksempel i kropsbårne kameraer, som i stigende grad bliver brugt i praksis.

(GDPR) og relevant national lovgivning[6]. Selv inden for rammerne af retshåndhævelsesdirektivet kan data, der behandles ved hjælp af teknologi til ansigtsgenkendelse, ud over autentifikations- eller identifikationsfunktionerne også viderebehandles til andre formål, f.eks. kategorisering.

17. Mere specifikt kan der opstilles en skala af potentielle anvendelser afhængigt af den grad af kontrol, folk har over deres personlige data, de effektive midler, de har til at udøve en sådan kontrol og deres ret til at tage initiativ til at udløse og bruge denne teknologi, konsekvenserne for dem (i tilfælde af genkendelse eller ikke-genkendelse) og omfanget af den behandling, der udføres. Ansigtsgenkendelse baseret på en skabelon, der er lagret på en personlig enhed (et chipkort eller en smartphone osv.), der tilhører den pågældende person, og som anvendes til autentifikation og udelukkende til personlig brug gennem et dedikeret interface, indebærer ikke de samme risici som f.eks. anvendelse til identifikationsformål i et ukontrolleret miljø uden aktiv inddragelse af de registrerede, hvor skabelonen for hvert ansigt, der kommer ind i overvågningsområdet, sammenlignes med skabeloner fra et bredt tværsnit af den population, der er lagret i en database. Mellem disse to yderpunkter ligger et meget varieret spektrum af anvendelser og dertil knyttede problemer i forbindelse med beskyttelse af personlige data.

18. For yderligere at illustrere den kontekst, inden for hvilken teknologier til ansigtsgenkendelse i øjeblikket drøftes eller implementeres, enten med henblik på autentifikation eller identifikation, finder Databeskyttelsesrådet det relevant at nævne en række eksempler. Eksemplerne nedenfor er udelukkende beskrivende og bør ikke betragtes som en form for foreløbig vurdering af deres overensstemmelse med EU's regelsæt inden for databeskyttelse.

Eksempler på autentifikation med ansigtsgenkendelse

19. Autentifikation kan designes, så brugerne har fuld kontrol over den, f.eks. for at give adgang til tjenester eller applikationer udelukkende i hjemmet. Som sådan anvendes det i vidt omfang af smartphoneejere til at låse deres enhed op i stedet for bekræftelse med adgangskode.

20. Ansigtsgenkendelse med autentifikation kan også bruges til at tjekke identiteten af en person, der ønsker at benytte offentlige eller private tredjepartstjenester. Sådanne processer tilbyder således en måde at skabe en digital identitet ved hjælp af en mobilapp (smartphone, tablet osv.), som derefter kan bruges til at få adgang til administrative tjenester online.

21. Desuden kan autentifikation med ansigtsgenkendelse have til formål at kontrollere fysisk adgang til et eller flere forudbestemte steder, såsom indgange til bygninger eller specifikke overgangssteder. Denne funktionalitet er f.eks. implementeret i visse behandlinger med henblik på grænsepassage, hvor personens ansigt ved kontrolstedet sammenlignes med det, der er gemt i den pågældendes identitetsdokument (pas eller sikker opholdstilladelse).

Eksempler på identifikation med ansigtsgenkendelse

22. Identifikation kan anvendes på mange og stadig mere forskelligartede måder. De omfatter især, men er ikke begrænset til, de anvendelser, der er anført nedenfor, som i øjeblikket er under observation, eksperimenteres med eller planlægges i EU:

    - søgning i en database med fotografier efter identiteten på en uidentificeret person (offer, mistænkt osv.)

[6] For yderligere vejledning, se også Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger, der blev vedtaget den 29. januar 2020.

- overvågning af en persons bevægelser i det offentlige rum. Hans eller hendes ansigt sammenlignes med de biometriske skabeloner for personer, der er i eller har været i det overvågede område, f.eks. når et stykke bagage efterlades, eller når der er begået en forbrydelse

- rekonstruktion af en persons bevægelser og efterfølgende interaktioner med andre personer gennem en forsinket sammenligning af disse elementer i et forsøg på f.eks. at identificere personens kontakter

- biometrisk fjernidentifikation af eftersøgte personer i det offentlige rum. Alle ansigter, der optages live af videoovervågningskameraer, krydstjekkes i realtid med en database, som sikkerhedsstyrkerne har adgang til

- automatisk genkendelse af personer på et billede for at identificere f.eks. deres relationer på et socialt netværk, som benytter teknologien. Billedet sammenlignes med skabelonerne for de personer på netværket, der har givet samtykke til denne funktionalitet, for at foreslå den nominative identifikation af disse relationer

- adgang til tjenester, hvor nogle pengeautomater kan genkende kunder ved at sammenligne et ansigt, der er optaget af et kamera, med bankens database over ansigtsbilleder

- sporing af en passagers bevægelser på et bestemt tidspunkt af et rejseforløb. Den skabelon, der beregnes i realtid for personer, der tjekker ind ved elektroniske kontroller, der er placeret på bestemte stadier af et rejseforløb (bagageafleveringssteder, boarding-gates osv.), sammenlignes med skabelonerne for personer, der tidligere er registreret i systemet.

23. Ud over selve brugen af ansigtsgenkendelsesteknologi inden for retshåndhævelse gør den brede vifte af applikationer, der er observeret, det klart, at en omfattende debat og politisk tilgang er nødvendig for at sikre sammenhæng og overholdelse af EU's regelsæt inden for databeskyttelse.

2.3 Pålidelighed, nøjagtighed og risici for de registrerede

24. Som enhver anden teknologi kan ansigtsgenkendelse også give udfordringer, når det kommer til iværksættelsen, især hvad angår dens pålidelighed og effektivitet med hensyn til autentifikation eller identifikation, såvel som det overordnede spørgsmål om kvalitet og nøjagtighed af "kildedata" og resultatet af behandling med ansigtsgenkendelsesteknologiske systemer.

25. Sådanne teknologiske udfordringer medfører særlige risici for de berørte registrerede, som er endnu mere betydningsfulde eller alvorlige inden for retshåndhævelse i betragtning af de mulige virkninger, retslige eller andre, for de registrerede, der kan blive påvirket i betydeligt omfang. I denne sammenhæng bør det også understreges, at en efterfølgende anvendelse af ansigtsgenkendelsesteknologi ikke i sig selv er sikrere, da personer kan spores på tværs af tid og steder. Efterfølgende anvendelse indebærer således også specifikke risici, som skal vurderes fra sag til sag[7].

26. Som Den Europæiske Unions Agentur for Grundlæggende Rettigheder påpeger i sin rapport fra 2019, "er det en udfordring at bestemme det nødvendige nøjagtighedsniveau for ansigtsgenkendelsessoftware: Der er mange forskellige måder at evaluere og vurdere nøjagtighed på, også afhængigt af opgaven, formålet og konteksten for brugen af den. Når man anvender teknologien på steder, der besøges af millioner af mennesker – såsom togstationer eller lufthavne – betyder en relativt lille andel af fejl (f.eks. 0,01 %)[8] stadig, at hundredvis af mennesker bliver markeret forkert.

[7] Se eksemplerne i bilag III.

[8] Denne nøjagtighedsrate stammer fra den citerede rapport og afspejler en rate, der er langt bedre end den nuværende ydeevne for de algoritmer, der anvendes inden for ansigtsgenkendelsesteknologi.

Desuden kan visse kategorier af personer være mere tilbøjelige til at blive matchet forkert end andre, som beskrevet i afsnit 3. Der er forskellige måder at beregne og fortolke fejlprocenterne på, så der skal udvises forsigtighed. Hvad angår nøjagtighed og fejl, er spørgsmål om, hvor let et system kan narres af f.eks. falske ansigtsbilleder (kaldet "spoofing"), desuden vigtigt, især i forbindelse med retshåndhævelse"[9].

27. I denne sammenhæng finder Databeskyttelsesrådet det vigtigt at minde om, at ansigtsgenkendelsesteknologi, uanset om denne teknologi bruges til autentifikation eller identifikation, ikke giver et endeligt resultat, men bygger på sandsynligheder for, at to ansigter eller billeder af ansigter svarer til den samme person[10]. Dette resultat forringes yderligere, når kvaliteten af de biometriske prøvers input til ansigtsgenkendelse er lav. Slørede inputbilleder, lav kameraopløsning, bevægelse og svagt lys kan være faktorer, der medfører lav kvalitet. Andre aspekter med betydelig indflydelse på resultaterne er prævalens og spoofing, f.eks. når kriminelle forsøger enten at undgå at passere kameraerne eller at narre ansigtsgenkendelsesteknologien. Talrige undersøgelser har også vist, at de statistiske resultater fra algoritmisk behandling kan indebære forudindtagethed, navnlig som følge af kildedatakvalitet eller træningsdatabaser eller andre faktorer såsom valget af sted for anvendelsen. Desuden bør indvirkningen af ansigtsgenkendelsesteknologi på andre grundlæggende rettigheder, såsom respekt for privat- og familieliv, ytrings- og informationsfrihed, forsamlings- og foreningsfrihed osv., også nævnes

28. Det er derfor afgørende, at der tages hensyn til ansigtsgenkendelsesteknologiens pålidelighed og nøjagtighed som kriterier ved vurderingen af overholdelsen af de centrale databeskyttelsesprincipper, jf. artikel 4 i retshåndhævelsesdirektivet, og navnlig når det drejer sig om retfærdighed og nøjagtighed.

29. Databeskyttelsesrådet fremhæver, at data af høj kvalitet er afgørende for algoritmer af høj kvalitet, men understreger også behovet for, at dataansvarlige som led i deres forpligtelse til ansvarlighed foretager en regelmæssig og systematisk evaluering af algoritmisk behandling for navnlig at sikre nøjagtighed, retfærdighed og pålidelighed af resultatet af denne behandling af personoplysninger. Personoplysninger, der anvendes til evaluering, træning og videreudvikling af systemer med ansigtsgenkendelsesteknologi, må kun behandles på grundlag af et tilstrækkeligt retsgrundlag og i overensstemmelse med de fælles databeskyttelsesprincipper.

3 GÆLDENDE RETLIGE RAMMER

30. Anvendelsen af teknologier til ansigtsgenkendelse er uløseligt forbundet med behandling af personoplysninger, herunder særlige kategorier af oplysninger. Desuden har det direkte eller indirekte indflydelse på en række grundlæggende rettigheder, som er nedfældet i EU's charter om grundlæggende rettigheder. Dette er særlig relevant inden for retshåndhævelse og strafferet. Derfor bør enhver brug af ansigtsgenkendelsesteknologier ske i nøje overensstemmelse med de gældende retlige rammer.

31. De følgende oplysninger bør tages under overvejelse i forbindelse med vurderingen af fremtidige lovgivningsmæssige og administrative foranstaltninger samt gennemførelsen af eksisterende lovgivning for hver enkelt sag, der involverer ansigtsgenkendelsesteknologi. Relevansen af de respektive krav varierer afhængigt af de særlige omstændigheder. Da ikke alle fremtidige

[9] Facial recognition technology: fundamental rights considerations in the context of law enforcement (Ansigtsgenkendelsesteknologi: overvejelser om grundlæggende rettigheder i forbindelse med retshåndhævelse), EU's Agentur for Grundlæggende Rettigheder, 21. november 2019.
[10] Denne sandsynlighed benævnes "konfidensscore".

omstændigheder kan forudses, er dette kun ment som en støtte og skal ikke forstås som en udtømmende opremsning.

3.1 Generel retlig ramme – EU's charter om grundlæggende rettigheder og den europæiske menneskerettighedskonvention (EMRK)

3.1.1 Chartrets anvendelighed

32. EU's charter om grundlæggende rettigheder (herefter "chartret") er rettet til Unionens institutioner, organer, kontorer og agenturer og til medlemsstaterne, når de gennemfører EU-lovgivning.

33. Regulering af behandlingen af biometriske data med henblik på retshåndhævelse i henhold til artikel 1, stk. 1, i retshåndhævelsesdirektivet rejser uundgåeligt spørgsmålet om overholdelse af de grundlæggende rettigheder, navnlig respekten for privatliv og kommunikation i henhold til artikel 7 i chartret og retten til beskyttelse af personoplysninger i henhold til artikel 8 i chartret.

34. Indsamling og analyse af videooptagelser af fysiske personer, herunder deres ansigter, indebærer behandling af personoplysninger. Ved teknisk behandling af billedet omfatter behandlingen også biometriske data. Teknisk behandling af oplysninger om en fysisk persons ansigt med hensyn til tid og sted gør det muligt at drage konklusioner vedrørende den pågældende persons privatliv. Sådanne konklusioner kan henvise til racemæssig eller etnisk oprindelse, sundhed, religion, hverdagsvaner, permanente eller midlertidige opholdssteder, daglige eller andre bevægelser, de aktiviteter, der udføres, disse personers sociale relationer og de sociale miljøer, som de færdes i. Den brede vifte af oplysninger, der kan afsløres ved anvendelsen af ansigtsgenkendelsesteknologi, viser klart den mulige indvirkning på retten til beskyttelse af personoplysninger, der er fastsat i chartrets artikel 8, men også på retten til privatlivets fred, der er fastsat i chartrets artikel 7.

35. Under sådanne omstændigheder er det heller ikke utænkeligt, at indsamling, analyse og den videre behandling af de pågældende biometriske (ansigts)data kan påvirke den måde, folk føler sig frie til at handle på, selv om handlingen ville være fuldt ud inden for rammerne af et frit og åbent samfund. Det kan også have alvorlige konsekvenser for udøvelsen af deres grundlæggende rettigheder såsom deres ret til tanke-, samvittigheds- og religionsfrihed, retten til frit at deltage i fredelige forsamlinger og foreningsfrihed i henhold til chartrets artikel 1, 10, 11 og 12. En sådan behandling indebærer også andre risici, såsom risikoen for misbrug af de personoplysninger, der indsamles af de relevante myndigheder, som følge af ulovlig adgang til og brug af personoplysninger, sikkerhedsbrud osv. Risiciene afhænger ofte af behandlingen og dens omstændigheder såsom risikoen for ulovlig adgang og behandling fra politimedarbejderes eller andre uautoriserede parters side. Men nogle risici er simpelthen iboende i de biometriske datas unikke natur. I modsætning til ændring af en adresse eller et telefonnummer kan en registreret ikke ændre vedkommendes entydige karakteristika, f.eks. ansigtet eller iris. I tilfælde af uautoriseret adgang eller utilsigtet offentliggørelse af biometriske data vil dette føre til, at oplysningerne kompromitteres i deres anvendelse som adgangskoder eller kryptografiske nøgler, eller at de kan anvendes til yderligere, uautoriserede overvågningsaktiviteter til skade for den registrerede.

3.1.2 Indgreb i de rettigheder, der er fastsat i chartret

36. Behandling af biometriske data udgør under alle omstændigheder et alvorligt indgreb i sig selv. Dette afhænger ikke af resultatet, f.eks. en positiv matchning. Behandlingen udgør et indgreb, selv om den biometriske skabelon slettes med det samme, efter at matchningen mod en politidatabase resulterer i et no-hit.

37. Indgrebet i de registreredes grundlæggende rettigheder kan skyldes en retsakt, der har til formål eller til følge at begrænse den pågældende grundlæggende rettighed[11]. Det kan også være resultatet af en handling foretaget af en offentlig myndighed med samme formål eller virkning eller endda af en privat enhed, der ved lov er betroet at udøve offentlig myndighed og offentlige beføjelser.

38. En lovgivningsmæssig foranstaltning, der tjener som retsgrundlag for behandling af personoplysninger, griber direkte ind i de rettigheder, der er sikret ved chartrets artikel 7 og 8[12].

39. Brugen af biometriske data og især ansigtsgenkendelsesteknologi påvirker i mange tilfælde også retten til menneskelig værdighed, som er sikret i artikel 1 i chartret. Menneskelig værdighed indebærer, at personer ikke blot behandles som objekter. Ansigtsgenkendelsesteknologi beregner de eksistentielle og meget personlige karakteristika, som ansigtstrækkene er, til en maskinlæsbar form med det formål at bruge denne form som en menneskelig nummerplade eller ID-kort, og derved objektiveres ansigtet.

40. En sådan behandling kan også gribe ind i andre grundlæggende rettigheder, såsom rettighederne i henhold til artikel 10, 11 og 12 i chartret, for så vidt som afskrækkende virkninger enten er tilsigtede eller stammer fra den relevante videoovervågning fra de retshåndhævende myndigheders side.

41. Derudover bør man også nøje overveje de potentielle risici, der er forbundet med retshåndhævende myndigheders brug af ansigtsgenkendelsesteknologier i forhold til retten til en retfærdig rettergang og uskyldsformodningen i henhold til artikel 47 og 48 i chartret. Resultatet af anvendelsen af ansigtsgenkendelsesteknologi, f.eks. et match, kan ikke kun føre til, at en person bliver udsat for yderligere politiarbejde, men også være afgørende bevismateriale i en retssag. Mangler i forbindelse med ansigtsgenkendelsesteknologi såsom mulig forudindtagethed, forskelsbehandling eller forkert identifikation ("falske positive") kan således også have alvorlige konsekvenser i straffesager. Desuden kan det ske, at man i vurderingen af beviser favoriserer resultatet af anvendelsen af ansigtsgenkendelsesteknologi, selv om der er modstridende beviser ("automatiseringsbias").

3.1.3 Begrundelser for indgreb

42. Ifølge chartrets artikel 52, stk. 1, skal enhver begrænsning i udøvelsen af grundlæggende rettigheder og frihedsrettigheder være fastlagt i lovgivningen og skal respektere disse rettigheders og frihedsrettigheders væsentligste indhold. Under iagttagelse af proportionalitetsprincippet kan der kun indføres begrænsninger, såfremt disse er nødvendige og faktisk svarer til mål af almen interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og frihedsrettigheder

3.1.3.1 Fastlagt i lovgivning

43. Chartrets artikel 52, stk. 1, fastsætter kravet om et specifikt retsgrundlag. Dette retsgrundlag skal være tilstrækkeligt klart formuleret til at give borgerne en passende indikation af de betingelser og omstændigheder, hvorunder myndighederne er bemyndiget til at anvende enhver form for indsamling af data og hemmelig overvågning[13]. Det skal med rimelig klarhed angive omfanget af og måden, hvorpå de offentlige myndigheder udøver den relevante skønsbeføjelse, således at enkeltpersoner sikres det minimum af beskyttelse, de har krav på i henhold til retsstatsprincippet i et demokratisk samfund[14]. Desuden indebærer lovlighed, at der kræves tilstrækkelige garantier for at sikre, at navnlig en enkeltpersons rettigheder i henhold til chartrets artikel 8 respekteres. Disse principper gælder også for

[11] Domstolen, sag C-219/91, Ter Voort, RoC 1992 I-05485, præmis 36 ff.; Domstolen, C-200/96, Metronome, RoC 1998 I-1953, præmis 28.
[12] Domstolen, sag C-594/12, præmis 36; Domstolen, sag C-291/12, præmis 23 ff.
[13] EMD, Shimovolos mod Rusland, præmis 68; Vukota-Bojić mod Schweiz.
[14] EMD, Piechowicz mod Polen, præmis 212.

behandling af personoplysninger med henblik på evaluering, træning og videreudvikling af systemer med ansigtsgenkendelsesteknologi.

44. Eftersom biometriske data, når de behandles med det formål entydigt at identificere en fysisk person, udgør en af de særlige kategorier af oplysninger, der er anført i artikel 10 i retshåndhævelsesdirektivet, vil de forskellige anvendelser af retshåndhævelsesdirektivet i de fleste tilfælde kræve en særskilt lov, der præcist beskriver applikationen og betingelserne for dens anvendelse. Dette omfatter især kriminalitetstyper og, hvor det er relevant, den passende tærskel for alvorligheden af disse forbrydelser, for bl.a. effektivt at udelukke småkriminalitet[15].

3.1.3.2 Essensen af den grundlæggende ret til privatlivets fred og til beskyttelse af personoplysninger, der er fastlagt i artikel 7 og 8 i chartret

45. Begrænsningerne af de grundlæggende rettigheder, der gælder for hver enkelt situation, skal stadig sikre, at essensen af den særlige rettighed respekteres. Essensen henviser til selve kernen af den relevante grundlæggende rettighed[16]. Den menneskelige værdighed skal også respekteres, selv når en rettighed er begrænset[17].

46. Tegn på en mulig krænkelse af den ukrænkelige kerne er følgende:

- En bestemmelse, der pålægger begrænsninger uafhængigt af en persons individuelle adfærd eller særlige omstændigheder[18].
- Indbringelse for domstolene er ikke muligt eller hindres[19].
- Forud for en alvorlig begrænsning tages der ikke hensyn til den pågældende persons omstændigheder[20].
- Med henblik på rettighederne i henhold til artikel 7 og 8 i chartret: Ud over en bred indsamling af metadata om kommunikation kan erhvervelse af viden om indholdet af den elektroniske kommunikation krænke essensen af disse rettigheder[21].
- Med henblik på rettighederne i henhold til artikel 7, 8 og 11 i chartret: Lovgivning, der kræver, at udbydere af adgang til offentlige onlinekommunikationstjenester og hostingtjenesteudbydere generelt og udifferentieret opbevarer bl.a. personoplysninger vedrørende disse tjenester[22].
- Med henvisning til rettighederne i henhold til artikel 8 i chartret: En mangel på grundlæggende principper for databeskyttelse og datasikkerhed kan også krænke kernen i retten[23].

3.1.3.3 Legitimt mål

47. Som allerede forklaret i afsnit 3.1.3. skal begrænsninger af de grundlæggende rettigheder reelt opfylde mål af almen interesse, der er anerkendt af Den Europæiske Union, eller opfylde behovet for at beskytte andres rettigheder og frihedsrettigheder.

---

[15] Se f.eks. Domstolens domme i sag C-817/19, Ligue des droits humains, præmis 151 ff., og sag C-207/16, Ministerio Fiscal, præmis 56.
[16] Domstolen, sag C-279/09, RoC 2010 I-13849, præmis 60.
[17] Forklaringer til chartret om grundlæggende rettigheder, afsnit I, forklaring til artikel 1 (EUT C 303 af 14.12.2007, s.17-35).
[18] Domstolen, sag C-601/15, præmis 52.
[19] Domstolen, sag C-400/10, RoC 2010 I-08965, præmis 55.
[20] Domstolen, sag C-408/03, RoC 2006 I-02647, præmis 68.
[21] Domstolen, sag C-203/15, Tele2 Sverige, præmis 101 med henvisning til Domstolen, sag C-293/12 og C-594/12, præmis 39.
[22] Domstolen, sag C-512/18, La Quadrature du Net, præmis 209 ff.
[23] Domstolen, sag C-594/12, præmis 40.

48. Anerkendt af Unionen er både de mål, der er nævnt i artikel 3 i traktaten om Den Europæiske Union, og andre interesser, der er beskyttet af specifikke bestemmelser i traktaterne[24], dvs. – bl.a. – et område med frihed, sikkerhed og retfærdighed samt forebyggelse og bekæmpelse af kriminalitet. Unionen bør i sine forbindelser med den øvrige verden bidrage til fred og sikkerhed og til beskyttelsen af menneskerettighederne.

49. Behovet for at beskytte andres rettigheder og frihedsrettigheder henviser til personers rettigheder, der er beskyttet af lovgivningen i Den Europæiske Union eller i dens medlemsstater. Vurderingen skal foretages med det formål at forene kravene til beskyttelse af de respektive rettigheder og at finde en rimelig balance mellem dem[25].

3.1.3.4 Nødvendigheds- og proportionalitetstest

50. Hvis der er tale om indgreb i de grundlæggende rettigheder, kan omfanget af den nationale lovgivers og EU-lovgiverens skønsbeføjelser vise sig at være begrænset. Dette afhænger af en række faktorer, herunder det pågældende område, arten af den pågældende rettighed, der er sikret ved chartret, arten og sværhedsgraden af indgrebet og det formål, der forfølges med indgrebet[26]. Lovgivningsmæssige foranstaltninger skal være passende for at nå de legitime mål, der forfølges af den pågældende lovgivning. Desuden må foranstaltningen ikke overskride grænserne for, hvad der er hensigtsmæssigt og nødvendigt for at nå disse mål[27]. Et mål af almen interesse – uanset hvor grundlæggende det måtte være – kan ikke i sig selv begrunde en begrænsning af en grundlæggende rettighed[28].

51. I henhold til Domstolens faste retspraksis må undtagelser og begrænsninger vedrørende beskyttelse af personoplysninger kun finde anvendelse, i det omfang det er strengt nødvendigt[29]. Dette indebærer også, at der ikke er mindre indgribende midler til rådighed til at nå målet. Mulige alternativer såsom – afhængigt af det givne formål – ekstra personale, hyppigere politikontrol eller yderligere vejbelysning skal identificeres og vurderes nøje. Lovgivningsmæssige foranstaltninger bør differentiere og målrette de personer, der er omfattet af dem, i lyset af målet, f.eks. bekæmpelse af grov kriminalitet. Hvis det dækker alle personer på en generel måde uden en sådan differentiering, begrænsning eller undtagelse, forstærker det indgrebet[30]. Det intensiverer også indgrebet, hvis databehandlingen omfatter en betydelig del af befolkningen[31].

52. Den beskyttelse af personoplysninger, der følger af den udtrykkelige forpligtelse i chartrets artikel 8, stk. 1, er særlig vigtig for retten til respekt for privatlivets fred, der er nedfældet i chartrets artikel 7[32]. Lovgivningen skal fastsætte klare og præcise regler for omfanget og anvendelsen af den pågældende foranstaltning og indføre sikkerhedsforanstaltninger, så de personer, hvis data er blevet behandlet,

---

[24] Forklaringer til chartret om grundlæggende rettigheder, afsnit I, forklaring til artikel 52 (EUT C 303 af 14.12.2007, s. 17-35).

[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31-32.

[26] Domstolen, sag C-594/12, præmis 47 med følgende kilder: se analogt, hvad angår artikel 8 i EMRK, Eur. Court H.R., S. og Marper mod Det Forenede Kongerige [GC], nr. 30562/04 og 30566/04, præmis 102, EMRK 2008-V.

[27] Domstolen, sag C-594/12, præmis 46 med følgende kilder: Sag C-343/09, Afton Chemical, EU:C:2010:419, præmis 45; Volker und Markus Schecke og Eifert, EU:C:2010:662, præmis 74; Sag C-581/10 og C-629/10, Nelson m.fl., EU:C:2012:657, præmis 71; Sag C-283/11 Sky Österreich, EU:C:2013:28, præmis 50; og sag C-101/12 Schaible, EU:C:2013:661, præmis 29.

[28] Domstolen, sag C-594/12, præmis 51.

[29] Domstolen, sag C-594/12, præmis 52, med følgende kilder: Sag C-473/12 IPI EU:C:2013:715, præmis 39 og den citerede retspraksis.

[30] Domstolen, sag C-594/12, præmis 57.

[31] Domstolen, sag C-594/12, præmis 56.

[32] Domstolen, sag C-594/12, præmis 53.

har tilstrækkelige garantier til effektivt at beskytte deres personlige data mod risikoen for misbrug og mod enhver ulovlig adgang til eller brug af disse data[33]. Behovet for sådanne sikkerhedsforanstaltninger er så meget desto større, når personoplysninger er genstand for automatisk behandling, og når der er en betydelig risiko for ulovlig adgang til oplysningerne[34]. Desuden kan intern eller ekstern, f.eks. retslig, godkendelse af anvendelsen af ansigtsgenkendelsesteknologi også bidrage som sikkerhedsforanstaltninger og kan vise sig at være nødvendig i visse tilfælde af alvorlig indgriben[35].

53. De fastlagte regler skal tilpasses den specifikke situation, f.eks. mængden af behandlede data, karakteren af data[36] og risikoen for ulovlig adgang til data. Dette forudsætter regler, der navnlig skal tjene til at regulere beskyttelsen og sikkerheden af de pågældende oplysninger på en klar og streng måde for at sikre deres fulde integritet og fortrolighed[37].

54. Med hensyn til forholdet mellem den dataansvarlige og databehandleren bør det ikke være tilladt for databehandlerne kun at tage hensyn til økonomiske overvejelser, når de fastlægger det sikkerhedsniveau, de anvender på personoplysninger; dette kunne bringe et tilstrækkeligt højt beskyttelsesniveau i fare[38].

55. En lov skal fastsætte materielle og proceduremæssige betingelser og objektive kriterier for at bestemme grænserne for de kompetente myndigheders adgang til data og deres efterfølgende brug. Med henblik på forebyggelse, afsløring eller strafferetlig forfølgning skal de pågældende lovovertrædelser anses for at være tilstrækkeligt alvorlige til at begrunde omfanget og alvoren af disse indgreb i de grundlæggende rettigheder, der er nedfældet i f.eks. chartrets artikel 7 og 8[39].

56. Oplysningerne skal behandles på en måde, der sikrer anvendeligheden og virkningen af EU's databeskyttelsesregler, navnlig dem, der er fastsat i chartrets artikel 8, hvori det hedder, at overholdelsen af kravene om beskyttelse og sikkerhed er underlagt en uafhængig myndigheds kontrol. Det geografiske sted, hvor behandlingen finder sted, kan i en sådan situation være relevant[40].

57. Med hensyn til de forskellige trin i behandlingen af personoplysninger bør der skelnes mellem kategorierne af oplysninger på grundlag af deres mulige nytteværdi med henblik på det mål, der forfølges, eller alt efter, hvilke personer der er berørt[41]. Fastlæggelsen af betingelserne for behandlingen, f.eks. fastsættelsen af opbevaringsperioden, skal baseres på objektive kriterier for at sikre, at indgrebet begrænses til det strengt nødvendige[42].

58. Ved vurderingen af nødvendighed og proportionalitet skal der på grundlag af hver enkelt situation identificeres og overvejes alle konsekvenser, der falder inden for anvendelsesområdet for andre

[33] Domstolen, sag C-594/12, præmis 54, med følgende kilder: se analogt, for så vidt angår artikel 8 i EMRK, Eur. Court H.R., Liberty m.fl. mod Det Forenede Kongerige, 1. juli 2008, nr. 58243/00, præmis 62 og 63; Rotaru mod Rumænien, præmis 57 til 59, og S. og Marper mod Det Forenede Kongerige, præmis 99.

[34] Domstolen, sag C-594/12, præmis 55, med følgende kilder: se analogt, for så vidt angår EMRK artikel 8, S. og Marper mod Det Forenede Kongerige, præmis 103, og M. K. mod Frankrig, 18. april 2013, nr. 19522/09, præmis 35.

[35] EMD, Szabó og Vissy mod Ungarn, præmis 73-77.

[36] Se også de skærpede krav til tekniske og organisatoriske foranstaltninger ved behandling af særlige kategorier af data, artikel 29, stk. 1, i retshåndhævelsesdirektivet.

[37] Domstolen, sag C-594/12, præmis 66.

[38] Domstolen, sag C-594/12, præmis 67.

[39] Domstolen, sag C-594/12, præmis 60 og 61.

[40] Domstolen, sag C-594/12, præmis 68.

[41] Domstolen, sag C-594/12, præmis 63.

[42] Domstolen, sag C-594/12, præmis 64.

grundlæggende rettigheder, såsom den menneskelige værdighed i henhold til chartrets artikel 1, retten til at tænke frit og til samvittigheds- og religionsfrihed i henhold til chartrets artikel 10, ytringsfrihed i henhold til chartrets artikel 11 samt forsamlings- og foreningsfrihed i henhold til chartrets artikel 12.

59. Desuden skal det betragtes som et spørgsmål af alvorlig karakter, at oplysninger, der systematisk behandles uden de registreredes vidende, sandsynligvis vil skabe en generel opfattelse af konstant overvågning[43]. Dette kan føre til afskrækkende virkninger med hensyn til nogle af eller alle de pågældende grundlæggende rettigheder.

60. For at lette og operationalisere vurderingen af nødvendighed og proportionalitet i lovgivningsmæssige foranstaltninger relateret til ansigtsgenkendelse på retshåndhævelsesområdet kunne de nationale lovgivere og EU-lovgiverne drage fordel af de tilgængelige praktiske værktøjer, der er specielt designet til denne opgave. Navnlig kan den nødvendigheds- og proportionalitetsværktøjskasse, som Den Europæiske Tilsynsførende for Databeskyttelse[44] stiller til rådighed, anvendes.

3.1.3.5 Artikel 52, stk. 3, og artikel 53 i chartret (beskyttelsesniveau, også i forhold til EMRK)

61. I henhold til artikel 52, stk. 3, og artikel 53 i chartret skal betydningen og omfanget af de rettigheder i chartret, der svarer til de rettigheder, der er sikret i EMRK, være de samme som dem, der er fastsat i EMRK. Selv om der navnlig for så vidt angår artikel 7 i chartret kan findes en tilsvarende bestemmelse i den europæiske menneskerettighedskonvention, er dette ikke tilfældet for chartrets artikel 8[45]. Chartrets artikel 52, stk. 3, forhindrer ikke EU-lovgivningen i at give en mere omfattende beskyttelse. Eftersom EMRK ikke udgør et retligt instrument, der formelt er blevet inkorporeret i EU-retten, skal EU-lovgivningen gennemføres i lyset af chartrets grundlæggende rettigheder[46].

62. I henhold til artikel 8 i EMRK må en offentlig myndighed ikke gribe ind i udøvelsen af denne ret til respekt for privatliv og familieliv, medmindre det er i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres ret og frihed.

63. EMRK fastsætter også standarder med hensyn til den måde, hvorpå begrænsninger kan gennemføres. Ét grundlæggende krav, ud over retsstatsprincippet, er forudsigelighed. Den nationale lovgivning skal være tilstrækkelig klar til at give borgere en tilstrækkelig tilkendegivelse, hvad angår de omstændigheder og forhold, hvorunder offentlige myndigheder er bemyndiget til at gribe til sådanne foranstaltninger[47]. Dette krav anerkendes af EU-Domstolen og EU's databeskyttelseslovgivning (jf. afsnit 3.2.1.1).

64. For yderligere at præcisere rettighederne i artikel 8 i EMRK skal bestemmelserne i konventionen om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af

[43] Domstolen, sag C-594/12, præmis 37.
[44] Den Europæiske Tilsynsførende for Databeskyttelse, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit (11.4.2017), Den Europæiske Tilsynsførende for Databeskyttelse: EDPS' Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019).
[45] Domstolen, sag C-203/15, Tele2 Sverige, præmis 129.
[46] Domstolen, sag C-311/18, præmis 99.
[47] Den Europæiske Menneskerettighedsdomstol, dom, Copland mod Det Forenede Kongerige, 03/04/2007, Application no. 62617/00, præmis 46.

personoplysninger[48] også respekteres fuldt ud. Alligevel skal det tages i betragtning, at disse bestemmelser kun repræsenterer en minimumsstandard i lyset af den gældende EU-lovgivning.

3.2 Specifik juridisk ramme – direktivet om retshåndhævelse

65. Der er fastsat en vis ramme for anvendelsen af ansigtsgenkendelsesteknologi i retshåndhævelsesdirektivet. For det første defineres begrebet "biometriske data" i artikel 3, nr. 13, i retshåndhævelsesdirektivet[49]. Se afsnit 2.1 ovenfor for yderligere detaljer. For det andet præciserer artikel 8, stk. 2, at for at en behandling kan være lovlig, skal den – ud over at være nødvendig til de formål, der er angivet i artikel 1, stk. 1 – være reguleret i national lovgivning, der som minimum skal angive målene med behandlingen, de personoplysninger, der skal behandles, og formålet med behandlingen. Yderligere bestemmelser af særlig relevans med hensyn til biometriske data er artikel 10 og 11 i retshåndhævelsesdirektivet. Artikel 10 skal læses i forbindelse med artikel 8 i retshåndhævelsesdirektivet[50]. Principperne for behandling af personoplysninger som fastlagt i artikel 4 i retshåndhævelsesdirektivet bør altid overholdes, og enhver vurdering af mulig biometrisk behandling via ansigtsgenkendelsesteknologi bør være styret af disse.

3.2.1 Behandling af særlige kategorier af data til retshåndhævelsesformål

66. I henhold til artikel 10 i retshåndhævelsesdirektivet er behandling af særlige kategorier af oplysninger såsom biometriske data kun tilladt, når det er strengt nødvendigt, og med forbehold af de fornødne garantier for den registreredes rettigheder og frihedsrettigheder. Derudover er det kun tilladt, hvis det er hjemlet i EU-retten eller medlemsstaternes nationale ret, for at beskytte den registreredes eller en anden fysisk persons vitale interesser, eller hvis en sådan behandling vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede. Denne generelle bestemmelse fremhæver følsomheden af behandlingen af særlige kategorier af oplysninger.

3.2.1.1 Hjemlet i EU-retten eller medlemsstaternes nationale ret

67. Med hensyn til den nødvendige type af lovgivningsmæssig foranstaltning hedder det i betragtning 33 i retshåndhævelsesdirektivet, at "når dette direktiv henviser til medlemsstaternes nationale ret, et retsgrundlag eller en lovgivningsmæssig foranstaltning, kræver det ikke nødvendigvis en lov, der er vedtaget af et parlament, med forbehold for krav i henhold til den forfatningsmæssige orden i den pågældende medlemsstat"[51].

68. I henhold til chartrets artikel 52, stk. 1, skal enhver begrænsning i udøvelsen af de rettigheder og frihedsrettigheder, der anerkendes ved chartret, være "fastlagt i lovgivningen". Dette afspejler udtrykket "i overensstemmelse med loven" i artikel 8, stk. 2, i den europæiske menneskerettighedskonvention, som ikke blot betyder overholdelse af national lovgivning, men også vedrører kvaliteten af denne lovgivning, og kræver, at den skal være i overensstemmelse med retsstatsprincippet.

---

[48] ETS nr. 108.

[49] Artikel 3, nr. 13), i retshåndhævelsesdirektivet: "Biometriske data" er personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger.

[50] WP258, Udtalelse om centrale spørgsmål i forbindelse med direktivet om retshåndhævelse (EU 2016/680), s. 7.

[51] Den type lovgivningsmæssige foranstaltninger, der overvejes, skal være i overensstemmelse med EU-retten eller med den nationale lovgivning. Afhængigt af begrænsningens grad af indgreb kan det være nødvendigt med en særlig lovgivningsmæssig foranstaltning på nationalt plan, der tager hensyn til normniveauet.

69. I betragtning 33 anføres det endvidere, at "en sådan national ret i medlemsstaterne, et sådant retsgrundlag eller en sådan lovgivningsmæssig foranstaltning bør imidlertid være klar(t) og præcis(t), og anvendelse heraf bør være forudsigelig for de personer, der er omfattet af dets/dens anvendelsesområde, jf. retspraksis fra Domstolen og Den Europæiske Menneskerettighedsdomstol. Medlemsstaternes nationale ret, som regulerer behandling af personoplysninger inden for dette direktivs anvendelsesområde, bør som minimum angive målene, de personoplysninger, der skal behandles, formålene med behandlingen og procedurerne for sikring af personoplysningernes integritet og fortrolighed samt procedurerne for deres tilintetgørelse".

70. Den nationale lovgivning skal være tilstrækkelig klart affattet til at give de registrerede tilstrækkelig viden om, under hvilke omstændigheder og forhold dataansvarlige er bemyndiget til at gribe til sådanne begrænsninger. Dette omfatter eventuelle forudsætninger for behandling såsom specifikke typer af bevismateriale samt nødvendigheden af retslige eller interne tilladelser. Den respektive lov kan være teknologineutral, så længe de specifikke risici og karakteristika ved behandlingen af persondata med systemer med ansigtsgenkendelsesteknologi er tilstrækkeligt præciseret. I overensstemmelse med retshåndhævelsesdirektivet og retspraksis fra Den Europæiske Unions Domstol (Domstolen) og Den Europæiske Menneskerettighedsdomstol (EMD) er det ganske rigtigt afgørende, at lovgivningsmæssige foranstaltninger, der har til formål at skabe et retsgrundlag for en foranstaltning til ansigtsgenkendelse, er forudsigelige for de registrerede.

71. En lovgivningsmæssig foranstaltning kan ikke påberåbes som en lov, der tillader behandling af biometriske data ved hjælp af ansigtsgenkendelsesteknologi med henblik på retshåndhævelse, hvis det blot er en gennemførelse af den generelle bestemmelse i retshåndhævelsesdirektivets artikel 10.

72. Bortset fra biometriske data regulerer artikel 10 i retshåndhævelsesdirektivet behandlingen af andre særlige kategorier af data, såsom seksuel orientering, politiske holdninger og religiøs overbevisning, og dækker dermed en bred vifte af behandlinger. Desuden ville en sådan bestemmelse mangle specifikke krav, der angiver de omstændigheder og betingelser, hvorunder de retshåndhævende myndigheder ville være bemyndiget til at bruge ansigtsgenkendelsesteknologi. På grund af henvisningen til andre typer data og det udtrykkelige behov for særlige sikkerhedsforanstaltninger uden yderligere specifikationer, kan en national bestemmelse, der omsætter artikel 10 i retshåndhævelsesdirektivet til national lovgivning – med en tilsvarende generel og abstrakt ordlyd – ikke påberåbes som retsgrundlag for behandling af biometriske data, der involverer ansigtsgenkendelse, da den ville mangle præcision og forudsigelighed. I overensstemmelse med artikel 28, stk. 2, eller artikel 46, stk. 1, litra c), i retshåndhævelsesdirektivet bør den nationale databeskyttelsestilsynsmyndighed høres, før lovgiveren skaber et nyt retsgrundlag for enhver form for behandling af biometriske data ved hjælp af ansigtsgenkendelse.

3.2.1.2 Strengt nødvendig

73. Behandling kan kun betragtes som "strengt nødvendig", hvis indgrebet i beskyttelsen af personoplysninger og begrænsningerne heraf er begrænset til, hvad der er absolut nødvendigt[52]. Tilføjelsen af ordet "strengt" betyder, at lovgiveren havde til hensigt, at behandlingen af særlige kategorier af data kun skulle finde sted under betingelser, der var endnu strengere end betingelserne for nødvendighed (se ovenfor, afsnit 3.1.3.4). Dette krav skal forstås som værende ufravigeligt. Det begrænser den skønsmargen, der er tilladt for den retshåndhævende myndighed i nødvendighedstesten, til et absolut minimum. I overensstemmelse med Domstolens faste retspraksis

[52] For konsistent retspraksis om den grundlæggende ret til respekt for privatlivet, se Domstolen, sag C-73/07, præmis 56 (Satakunnan Markkinapörssi og Satamedia); sag C-92/09 og C-93/09, præmis 77 (Schecke og Eifert); sag C-594/12, præmis 52 (digitale rettigheder); sag C-362/14, præmis 92 (Schrems).

er betingelsen om "streng nødvendighed" også tæt forbundet med kravet om objektive kriterier for at definere de omstændigheder og betingelser, hvorunder behandling kan foretages, hvilket udelukker enhver behandling af generel eller systematisk karakter[53].

3.2.1.3 Tydeligvis offentliggjort

74. Ved vurderingen af, om behandlingen vedrører oplysninger, som tydeligvis er offentliggjort af en registreret, bør det erindres, at et fotografi som sådant ikke systematisk betragtes som biometriske data[54]. Det faktum, at et fotografi tydeligvis er blevet offentliggjort af den registrerede, medfører derfor ikke, at de relaterede biometriske data, som kan hentes fra fotografiet med specifikke tekniske midler, anses for at være blevet tydeligvis offentliggjort.

75. Som for personoplysninger generelt skal den registrerede bevidst have gjort den biometriske skabelon (og ikke blot et ansigtsbillede) frit tilgængelig og offentlig via en åben kilde, for at biometriske data kan betragtes som tydeligvis offentliggjorte af den registrerede. Hvis en tredjepart videregiver de biometriske data, kan det ikke antages, at oplysningerne tydeligvis er blevet offentliggjort af den registrerede.

76. Desuden er det ikke tilstrækkeligt at fortolke den registreredes adfærd for at vurdere, at biometriske data tydeligvis er blevet offentliggjort. I tilfælde af sociale netværk eller onlineplatforme mener Databeskyttelsesrådet således, at det faktum, at den registrerede ikke har udløst eller indstillet specifikke privatlivsfunktioner, ikke er tilstrækkeligt til at anse, at denne registrerede tydeligvis har offentliggjort sine personlige data, og at disse data (f.eks. fotografier) kan behandles til biometriske skabeloner og bruges til identifikationsformål uden den registreredes samtykke. Mere generelt bør en tjenestes standardindstillinger, f.eks. at gøre skabeloner offentligt tilgængelige, eller manglende valgmuligheder, f.eks. at skabelonerne gøres offentligt tilgængelige, uden at brugeren kan ændre denne indstilling, ikke på nogen måde fortolkes som data, der tydeligvis er offentliggjort.

3.2.2 Automatiske individuelle afgørelser, herunder profilering

77. I retshåndhævelsesdirektivets artikel 11, stk. 1, fastsættes medlemsstaternes pligt til generelt at forbyde afgørelser, der alene er baseret på automatisk behandling, herunder profilering, og som har negative retsvirkninger for den registrerede eller påvirker den pågældende betydeligt. Som en undtagelse fra dette generelle forbud kan en sådan behandling kun være mulig, hvis den er hjemlet i EU-retten eller medlemsstaternes nationale ret, som den dataansvarlige er underlagt, og som fastsætter de fornødne garantier for den registreredes rettigheder og frihedsrettigheder, i det mindste den registreredes ret til menneskelig indgriben fra den dataansvarliges side. Den må kun anvendes restriktivt. Denne tærskel gælder for almindelige (dvs. ikke særlige) kategorier af personoplysninger. En endnu højere tærskel og mere restriktiv anvendelse gælder for fritagelsen i henhold til retshåndhævelsesdirektivets artikel 11, stk. 2. Det understreger på ny, at afgørelser i henhold til stk. 1 ikke må baseres på særlige kategorier af oplysninger, dvs. navnlig biometriske data, med det formål entydigt at identificere en fysisk person. Der kan kun indføres en undtagelse, hvis der er indført passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt den berørte fysiske persons legitime interesser. Denne undtagelse skal læses i tillæg til og i lyset af forudsætningerne i artikel 10 i retshåndhævelsesdirektivet.

---

[53] Domstolen, sag C--623/17, præmis 78.

[54] Jf. betragtning 51 i GDPR: "Behandling af fotografier bør ikke systematisk anses for at være behandling af særlige kategorier af personoplysninger, eftersom de kun vil være omfattet af definitionen af biometriske data, når de behandles ved en specifik teknisk fremgangsmåde, der muliggør entydig identifikation eller autentifikation af en fysisk person. "

78. Afhængigt af systemet for ansigtsgenkendelsesteknologi giver selv menneskelig indgriben ved vurderingen af resultaterne af ansigtsgenkendelsesteknologi ikke nødvendigvis i sig selv en tilstrækkelig garanti med hensyn til at respektere enkeltpersoners rettigheder og navnlig retten til beskyttelse af personoplysninger i betragtning af mulig forudindtagethed og fejl, der kan opstå som følge af selve behandlingen. Desuden kan menneskelig indgriben kun betragtes som en sikkerhedsforanstaltning, hvis den person, der griber ind, kritisk kan udfordre resultaterne af ansigtsgenkendelsesteknologien under den menneskelige indgriben. Det er afgørende at sætte personen i stand til at forstå systemet for ansigtsgenkendelsesteknologi og dets begrænsninger samt at fortolke dets resultater korrekt. Det er også nødvendigt at etablere en arbejdsplads og en organisation, der modvirker effekten af automatiseringsbias og undgår at fremme en ukritisk accept af resultaterne, f.eks. på grund af tidspres, besværlige procedurer, potentielle skadelige karriereeffekter osv.

79. I henhold til artikel 11, stk. 3, i retshåndhævelsesdirektivet er profilering, der fører til forskelsbehandling af fysiske personer på grundlag af særlige kategorier af personoplysninger såsom biometriske data, forbudt i henhold til EU-retten. I henhold til retshåndhævelsesdirektivets artikel 3, nr. 4), forstås ved "profilering" enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser Ved vurderingen af, om der er forudset passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt den berørte fysiske persons legitime interesser, skal der tages hensyn til, at brugen af ansigtsgenkendelsesteknologi kan føre til profilering afhængigt af den måde og det formål, som ansigtsgenkendelsesteknologien anvendes på. I overensstemmelse med EU-retten og artikel 11, stk. 3, i retshåndhævelsesdirektivet er profilering, der fører til forskelsbehandling af fysiske personer på grundlag af særlige kategorier af personoplysninger, under alle omstændigheder forbudt.

3.2.3 Kategorier af registrerede

80. Artikel 6 i retshåndhævelsesdirektivet omhandler nødvendigheden af at sondre mellem forskellige kategorier af registrerede. Denne sondring skal foretages, hvor det er relevant og så vidt det er muligt. Dens virkning skal fremgå af den måde, hvorpå oplysningerne behandles. Ud fra eksemplerne i artikel 6 i retshåndhævelsesdirektivet kan det udledes, at behandlingen af personoplysninger som hovedregel skal opfylde kriterierne om nødvendighed og proportionalitet, også med hensyn til kategorien af registrerede[55]. Det kan endvidere udledes, at for så vidt angår registrerede, for hvilke der ikke foreligger beviser, der kan tyde på, at deres adfærd kan have en forbindelse, selv indirekte eller fjern, med det legitime formål i overensstemmelse med retshåndhævelsesdirektivet, er der højst sandsynligt ingen begrundelse for et indgreb[56]. Hvis ingen sondring i henhold til artikel 6 i retshåndhævelsesdirektivet er anvendelig eller mulig, skal undtagelsen fra reglen i artikel 6 i retshåndhævelsesdirektivet nøje overvejes i vurderingen af nødvendigheden og proportionaliteten af indgrebet. Sondringen mellem forskellige kategorier af registrerede synes at være et væsentligt krav, når det kommer til behandling af personoplysninger, der involverer ansigtsgenkendelse, også i betragtning af de mulige falske positive eller falske negative resultater, som kan have betydelige konsekvenser for registrerede såvel som i løbet af en undersøgelse.

[55] Jf. også Domstolen, sag C-594/12, præmis 56-59.
[56] Jf. også Domstolen, sag C-594/12, præmis 58.

81. Som nævnt skal bestemmelserne i Den Europæiske Unions charter om grundlæggende rettigheder respekteres i forbindelse med gennemførelsen af EU-retten, jf. chartrets artikel 52. De rammer og kriterier, som retshåndhævelsesdirektivet fastlægger, skal derfor læses i lyset af chartret. EU's og dets medlemsstaters lovgivning må ikke falde under dette mål og skal sikre chartrets fulde virkning.

3.2.4 Den registreredes rettigheder

82. Databeskyttelsesrådet har allerede givet vejledning om registreredes rettigheder i henhold til GDPR i forskellige aspekter[57]. Retshåndhævelsesdirektivet indeholder bestemmelser om lignende rettigheder for registrerede, og der er givet generel vejledning herom i en udtalelse fra Artikel 29-Gruppen, som er blevet godkendt af Databeskyttelsesrådet[58]. Under visse omstændigheder giver retshåndhævelsesdirektivet mulighed for visse begrænsninger af disse rettigheder. Parametrene for sådanne begrænsninger vil blive uddybet nærmere i afsnit 3.2.4.6. "Legitime begrænsninger af den registreredes rettigheder".

83. Mens alle registreredes rettigheder, som er anført i kapitel III i retshåndhævelsesdirektivet, naturligvis også gælder for behandling af personoplysninger via ansigtsgenkendelsesteknologi, vil det følgende kapitel fokusere på nogle af de rettigheder og aspekter, som kan være særlig interessant at modtage vejledning om. Desuden forudsætter dette kapitel og dets analyse, at den pågældende behandling via ansigtsgenkendelsesteknologi har bestået de juridiske krav, som er beskrevet i det foregående kapitel.

84. I betragtning af karakteren af behandlingen af personoplysninger via ansigtsgenkendelsesteknologi (behandling af særlige kategorier af personoplysninger ofte uden nogen klar interaktion med den registrerede) skal den dataansvarlige nøje overveje, hvordan kravene i retshåndhævelsesdirektivet kan opfyldes (eller om det overhovedet er muligt), inden en behandling med ansigtsgenkendelsesteknologi iværksættes. Den dataansvarlige skal navnlig nøje analysere:

- hvem de registrerede er (ofte flere end den eller de personer, der er det primære mål for behandlingen)
- hvordan de registrerede gøres bekendt med behandlingen med ansigtsgenkendelsesteknologi (se afsnit 3.2.4.1)
- hvordan de registrerede kan udøve deres rettigheder (her kan både informations- og indsigtsrettigheder samt rettigheder til berigtigelse eller begrænsning være særligt udfordrende at opretholde, hvis ansigtsgenkendelsesteknologi bruges til alt andet end 1:1-verifikation i direkte kontakt med den registrerede).

3.2.4.1 Registrerede gøres bekendt med rettigheder og modtager oplysning i en kortfattet, letforståelig og lettilgængelig form.

85. Ansigtsgenkendelsesteknologi skaber udfordringer med hensyn til at sikre, at registrerede gøres bekendt med, at deres biometriske data behandles. Det er særligt udfordrende, hvis en retshåndhævende myndighed analyserer via videomateriale til brug for ansigtsgenkendelsesteknologi, der stammer fra eller er stillet til rådighed af en tredjepart, da den retshåndhævende myndighed kun har ringe – og for det meste ingen – mulighed for at underrette den registrerede på indsamlingstidspunktet (f.eks. via skiltning på stedet). Alt videomateriale, der ikke er relevant for efterforskningen (eller formålet med behandlingen), bør altid fjernes eller anonymiseres (f.eks. ved sløring uden mulighed for at gendanne dataene med tilbagevirkende kraft), før der foretages

[57] Se f.eks. Databeskyttelsesrådets retningslinjer 1/2022 om registreredes rettigheder – ret til indsigt, og 3/2019 om brug af videoudstyr til behandling af personoplysninger.
[58] WP258, Udtalelse om centrale spørgsmål i forbindelse med direktivet om retshåndhævelse (EU 2016/680).

behandling af biometriske data, for at undgå risikoen for ikke at have opfyldt minimeringsprincippet i artikel 4, stk. 1, litra e), og oplysningsforpligtelserne i artikel 13, stk. 2, i retshåndhævelsesdirektivet. Det er den dataansvarliges ansvar at vurdere, hvilke oplysninger der vil være af betydning for den registrerede i forbindelse med udøvelsen af vedkommendes rettigheder, og at sikre, at de nødvendige oplysninger gives. Den effektive udøvelse af den registreredes rettigheder er afhængig af, at den dataansvarlige opfylder sine oplysningsforpligtelser.

86. Artikel 13, stk. 1, i retshåndhævelsesdirektivet fastsætter, hvilke minimumsoplysninger der generelt skal stilles til rådighed for den registrerede. Disse oplysninger kan stilles til rådighed via den dataansvarliges websted, i trykt form (f.eks. en folder, der kan rekvireres) eller på en anden måde, der er let tilgængelig for den registrerede. Den dataansvarlige skal under alle omstændigheder sikre, at der effektivt oplyses om mindst følgende elementer:

- identitet og kontaktoplysninger for den dataansvarlige, også databeskyttelsesrådgiveren
- formålet med behandlingen, og at det er behandling via ansigtsgenkendelsesteknologi
- retten til at indgive en klage til en tilsynsmyndighed og kontaktoplysninger på denne myndighed
- retten til at anmode om adgang til og berigtigelse eller sletning af personoplysninger og begrænsning af behandling af personoplysninger.

87. I særlige tilfælde, der er defineret i national lovgivning, og som bør være i overensstemmelse med artikel 13, stk. 2, i retshåndhævelsesdirektivet[59], som f.eks. behandling via ansigtsgenkendelsesteknologi, skal følgende oplysninger desuden gives direkte til den registrerede:

- retsgrundlaget for behandlingen
- oplysninger om, hvor personoplysningerne blev indsamlet uden den registreredes viden
- det tidsrum, som personoplysningerne opbevares i, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum
- hvor det er relevant, kategorierne af modtagere af personoplysningerne (herunder i tredjelande eller internationale organisationer).

88. Mens artikel 13, stk. 1, i retshåndhævelsesdirektivet omhandler generelle oplysninger, der gøres tilgængelige for offentligheden, vedrører artikel 13, stk. 2, de yderligere oplysninger, der skal gives til en bestemt registreret i særlige tilfælde, f.eks. hvor oplysninger indsamles direkte fra den registrerede eller indirekte uden den registreredes viden[60]. Der er ingen klar definition af, hvad der menes med "særlige tilfælde" i artikel 13, stk. 2, i retshåndhævelsesdirektivet. Det refererer imidlertid til situationer, hvor de registrerede skal gøres opmærksom på den behandling, der vedrører dem specifikt, og gives passende oplysninger, så de effektivt kan udøve deres rettigheder. Databeskyttelsesrådet mener, at der ved vurderingen af, om der foreligger "et særligt tilfælde", skal tages hensyn til flere faktorer, herunder om personoplysninger indsamles uden den registreredes viden, da dette ville være den eneste måde, hvorpå de registrerede effektivt kan udøve deres rettigheder. Andre eksempler på "særlige tilfælde" kunne være, hvor personoplysninger behandles yderligere som genstand for en international strafferetlig samarbejdsprocedure eller i situationer, hvor

[59] F.eks. artikel 56, stk. 1, i den tyske forbundslov om databeskyttelse, som bl.a. fastsætter, hvilke oplysninger der skal gives til registrerede i undercover-operationer.
[60] WP258 Udtalelse om centrale spørgsmål i forbindelse med direktivet om retshåndhævelse (EU 2016/680), s.17-18.

personoplysninger behandles under hemmelige operationer som specificeret i national lovgivning. Desuden følger det af betragtning 38 i retshåndhævelsesdirektivet, at hvis beslutningstagningen udelukkende er baseret på ansigtsgenkendelsesteknologi, skal de registrerede informeres om funktionerne i den automatiserede beslutningstagning. Dette synes også at indikere, at dette er et særligt tilfælde, hvor der skal gives yderligere oplysninger til den registrerede i overensstemmelse med artikel 13, stk. 2, i retshåndhævelsesdirektivet[61].

89. Endelig skal det bemærkes, at medlemsstaterne i henhold til artikel 13, stk. 3, i retshåndhævelsesdirektivet kan vedtage lovgivningsmæssige foranstaltninger, der begrænser forpligtelsen til at give oplysninger i specifikke tilfælde for bestemte mål. Dette gælder i det omfang og så længe en sådan foranstaltning udgør en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund under behørigt hensyn til den berørte fysiske persons grundlæggende rettigheder og legitime interesser.

3.2.4.2 Ret til indsigt

90. Generelt har den registrerede ret til at modtage en positiv eller negativ bekræftelse af enhver behandling af hans eller hendes personoplysninger og, hvis svaret er positivt, adgang til personoplysningerne som sådan plus yderligere oplysninger, som anført i artikel 14 i retshåndhævelsesdirektivet. For ansigtsgenkendelsesteknologi bør dette, når biometriske data lagres og forbindes til en identitet, også ved hjælp af alfanumeriske data, give den kompetente myndighed mulighed for at bekræfte en anmodning om adgang baseret på en søgning ved hjælp af disse alfanumeriske data og uden at indlede yderligere behandling af andres biometriske data (dvs. ved at søge med ansigtsgenkendelsesteknologi i en database). Princippet om dataminimering skal overholdes, og der må ikke opbevares flere oplysninger end det, der er nødvendigt med hensyn til formålet med behandlingen.

3.2.4.3 Ret til berigtigelse af personoplysninger

91. Eftersom ansigtsgenkendelsesteknologi ikke sikrer absolut nøjagtighed, er det særlig vigtigt, at de dataansvarlige er opmærksomme på anmodninger om berigtigelse af personoplysninger. Det kan også være tilfældet, når en registreret baseret på ansigtsgenkendelsesteknologi er blevet placeret i en unøjagtig kategori, f.eks. uretmæssigt placeret i kategorien mistænkte baseret på en indledende antagelse om handlingsforløbet i en videooptagelse. Risiciene for de registrerede er særligt alvorlige, hvis sådanne unøjagtige oplysninger lagres i en politidatabase og/eller deles med andre enheder. Den dataansvarlige skal korrigere lagrede data og systemer med ansigtsgenkendelsesteknologi i overensstemmelse hermed, jf. betragtning 47 i retshåndhævelsesdirektivet.

3.2.4.4 Ret til sletning

92. Ansigtsgenkendelsesteknologi vil under de fleste omstændigheder – når det ikke gælder 1:1-verifikation/-autentifikation – indebære behandling af et stort antal registreredes biometriske data. Det er derfor vigtigt, at den dataansvarlige på forhånd overvejer, hvor grænserne for formålet og nødvendigheden ligger, så en anmodning om sletning i henhold til artikel 16 i retshåndhævelsesdirektivet kan behandles uden unødig forsinkelse (eftersom den dataansvarlige bl.a. har brug for at slette personoplysninger, der behandles ud over, hvad gældende lovgivning, der vedtages i henhold til artikel 4, 8 og 10 i retshåndhævelsesdirektivet giver mulighed for).

[61] Bemærk klart forskellen mellem "stilles til rådighed for eller gives den registrerede" i artikel 13, stk. 1, i retshåndhævelsesdirektivet og "skal gives den registrerede" i artikel 13, stk. 2, i retshåndhævelsesdirektivet. I artikel 13, stk. 2, i retshåndhævelsesdirektivet skal den dataansvarlige sikre, at oplysningerne når frem til den registrerede, og offentliggjorte oplysninger på en webside vil ikke være tilstrækkelige.

3.2.4.5 Ret til begrænsning

93. Hvis oplysningernes rigtighed bestrides af den registrerede, og oplysningernes rigtighed ikke kan fastslås (eller hvis personoplysningerne skal bevares som fremtidigt bevismiddel), har den dataansvarlige pligt til at begrænse den registreredes personoplysninger i overensstemmelse med artikel 16 i retshåndhævelsesdirektivet. Dette bliver især vigtigt, når det drejer sig om ansigtsgenkendelsesteknologi (baseret på en eller flere algoritmer og derved aldrig med et endeligt resultat) i situationer, hvor der indsamles store mængder data, og hvor nøjagtigheden og kvaliteten af identifikationen kan variere. Med videomateriale af dårlig kvalitet (f.eks. fra et gerningssted) øges risikoen for falske positive resultater. Endvidere gælder det, at hvis ansigtsbilleder på en observationsliste ikke opdateres regelmæssigt, vil dette også øge risikoen for falske positive eller falske negative resultater. I særlige tilfælde, hvor data ikke kan slettes, fordi der er rimelig grund til at tro, at sletning kan påvirke den registreredes legitime interesser, bør dataene i stedet begrænses og kun behandles til det formål, der forhindrede sletning (se betragtning 47 i retshåndhævelsesdirektivet).

3.2.4.6 Legitime begrænsninger af de registreredes rettigheder

94. Når det gælder den dataansvarliges oplysningsforpligtelser og de registreredes ret til indsigt, er begrænsninger kun tilladt, så længe de er fastsat i loven, som igen skal udgøre en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund under behørig hensyntagen til den berørte fysiske persons grundlæggende rettigheder og legitime interesser (se artikel 13, stk. 3, artikel 13, stk. 4, artikel 15 og artikel 16, stk. 4, i retshåndhævelsesdirektivet). Når ansigtsgenkendelsesteknologi anvendes til retshåndhævelsesformål, kan man forvente, at den vil blive anvendt under omstændigheder, hvor det ville være skadeligt for det forfulgte formål at underrette den registrerede eller give adgang til oplysningerne. Dette vil f.eks. gælde for en politiefterforskning af en forbrydelse eller for at beskytte den nationale sikkerhed eller den offentlige sikkerhed.

95. Retten til indsigt betyder ikke automatisk adgang til alle oplysningerne, f.eks. i en straffesag, hvor ens personoplysninger forekommer. Et brugbart eksempel på, hvornår begrænsninger af retten kan tillades, kunne være i løbet af en kriminel efterforskning.

3.2.4.7 Udøvelse af rettigheder gennem tilsynsmyndigheden

96. I de tilfælde, hvor der er legitime begrænsninger for udøvelsen af rettigheder i henhold til kapitel III i retshåndhævelsesdirektivet, kan den registrerede anmode databeskyttelsesmyndigheden om på den registreredes vegne at udøve sine rettigheder ved at kontrollere lovligheden af den dataansvarliges behandling. Det påhviler den dataansvarlige at underrette den registrerede om muligheden for at udøve sine rettigheder på denne måde (se artikel 17 og artikel 46, stk. 1, litra g), i retshåndhævelsesdirektivet). For ansigtsgenkendelsesteknologi betyder det, at den dataansvarlige skal sikre, at der er truffet passende foranstaltninger, således at en sådan anmodning kan behandles, f.eks. ved at gøre det muligt at søge efter registreret materiale, forudsat at den registrerede giver tilstrækkelige oplysninger til at lokalisere vedkommendes personoplysninger.

3.2.5 Andre juridiske krav og sikkerhedsforanstaltninger

3.2.5.1 Artikel 27 – Konsekvensanalyse vedrørende databeskyttelse

97. En konsekvensanalyse vedrørende databeskyttelse inden anvendelsen af ansigtsgenkendelsesteknologi er et obligatorisk krav, da typen af behandling, navnlig ved anvendelse af nye teknologier, og under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Eftersom anvendelsen af ansigtsgenkendelsesteknologi indebærer systematisk automatisk behandling af særlige kategorier af oplysninger, kan det antages, at den dataansvarlige i sådanne tilfælde som hovedregel vil være forpligtet til at foretage en konsekvensanalyse vedrørende databeskyttelse.

Konsekvensanalysen vedrørende databeskyttelse bør som minimum indeholde en generel beskrivelse af de påtænkte behandlingsaktiviteter, en vurdering af nødvendigheden og proportionaliteten af behandlingsaktiviteterne i forhold til formålene, en vurdering af risiciene for registreredes rettigheder og frihedsrettigheder, de foranstaltninger, der påtænkes for at imødegå disse risici, garantier, sikkerhedsforanstaltninger og mekanismer til at sikre beskyttelsen af personoplysninger og påvise overholdelse. Databeskyttelsesrådet anbefaler at offentliggøre resultaterne af sådanne vurderinger, eller i det mindste de vigtigste resultater og konklusioner af konsekvensanalysen vedrørende databeskyttelse som en tillids- og gennemsigtighedsforbedrende foranstaltning[62].

3.2.5.2 Artikel 28 – Forudgående høring af tilsynsmyndigheden

98. I henhold til artikel 28 i retshåndhævelsesdirektivet skal den dataansvarlige eller databehandleren høre tilsynsmyndigheden forud for behandlingen, såfremt: a) en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til en høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen, eller b) den type behandling, navnlig ved brug af nye teknologier, mekanismer eller procedurer, indebærer en høj risiko for de registreredes rettigheder og frihedsrettigheder. Som allerede forklaret i afsnit 2.3. i disse retningslinjer mener Databeskyttelsesrådet, at de fleste tilfælde af indførelse og anvendelse af ansigtsgenkendelsesteknologi indeholder en iboende høj risiko for de registreredes rettigheder og frihedsrettigheder. Derfor bør den myndighed, der indfører ansigtsgenkendelsesteknologi, ud over konsekvensanalysen vedrørende databeskyttelse høre den kompetente tilsynsmyndighed forud for indførelsen af systemet.

3.2.5.3 Artikel 29 – Behandlingssikkerhed

99. De biometriske datas entydige karakter gør det umuligt for en registreret at ændre dem, hvis de bliver kompromitteret, f.eks. som følge af et brud på datasikkerheden. Derfor bør den kompetente myndighed, der gennemfører og/eller anvender ansigtsgenkendelsesteknologi være særlig opmærksom på behandlingssikkerheden i overensstemmelse med artikel 29 i retshåndhævelsesdirektivet. Den retshåndhævende myndighed skal især sikre, at systemet overholder de relevante standarder og implementerer biometriske skabelonbeskyttelsesforanstaltninger[63]. Denne forpligtelse er endnu mere relevant, hvis den retshåndhævende myndighed bruger en tredjepart som tjenesteudbyder (databehandler).

3.2.5.4 Artikel 20 – Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

100. Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i overensstemmelse med artikel 20 i retshåndhævelsesdirektivet har til formål at sikre, at databeskyttelsesprincipper og -garantier, såsom dataminimering og lagringsbegrænsning, er integreret i teknologien gennem passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, selv inden behandlingen af personoplysninger påbegyndes, og at de vil blive anvendt gennem hele dens livscyklus. I betragtning af den iboende høje risiko for fysiske personers rettigheder og frihedsrettigheder bør valget af sådanne foranstaltninger ikke udelukkende afhænge af økonomiske overvejelser[64], men der bør i stedet stræbes efter at implementere de bedste databeskyttelsesteknologier. På samme måde skal en retshåndhævende myndighed, hvis den har til hensigt at iværksætte og anvende ansigtsgenkendelsesteknologi fra eksterne leverandører, f.eks. gennem udbudsprocedurer, sikre, at der kun anvendes ansigtsgenkendelsesteknologi, der bygger på

[62] Yderligere oplysninger kan findes i WP248 rev.01, Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko".
[63] Jf. f.eks.: ISO/IEC 24745 Informationssikkerhed, cybersikkerhed og privatlivsbeskyttelse – Beskyttelse af biometrisk information.
[64] Se betragtning 53 i retshåndhævelsesdirektivet.

principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger[65]. Dette indebærer også, at gennemsigtigheden med hensyn til, hvordan ansigtsgenkendelsesteknologi fungerer, ikke begrænses af påstande om forretningshemmeligheder eller intellektuelle ejendomsrettigheder.

3.2.5.5 Artikel 25 – Logning

101. Retshåndhævelsesdirektivet foreskriver forskellige metoder, hvorpå den dataansvarlige eller databehandleren kan påvise lovligheden af behandlingen og sikre dataintegritet og datasikkerhed. I den forbindelse er systemlogs et meget nyttigt værktøj og en vigtig sikkerhedsforanstaltning til verificering af lovligheden af behandlingen, både internt (dvs. egenkontrol) og fra eksterne tilsynsmyndigheders side, såsom databeskyttelsesmyndighederne. I henhold til artikel 25 i retshåndhævelsesdirektivet skal logfiler for mindst følgende behandlingsaktiviteter opbevares i automatiserede behandlingssystemer: indsamling, ændring, søgning, videregivelse, herunder overførsler, samkøring og sletning. Desuden bør logfilerne over søgning og videregivelse gøre det muligt at fastslå begrundelsen, datoen og tidspunktet for sådanne operationer og, så vidt muligt, identifikationen af den person, der konsulterede eller videregav personoplysninger, og identiteten af modtagerne af sådanne personoplysninger. I forbindelse med systemer til ansigtsgenkendelse anbefales det desuden at logge følgende yderligere behandlingsaktiviteter (delvis ud over artikel 25 i retshåndhævelsesdirektivet):

- ændringer af referencedatabasen (tilføjelse, sletning eller opdatering). Loggen bør opbevare en kopi af det relevante (tilføjede, slettede eller opdaterede) billede, når det ikke på anden måde er muligt at verificere lovligheden eller resultatet af behandlingsaktiviteterne.

- identifikations- eller verifikationsforsøg, herunder resultat og konfidensscore. Der bør gælde et strengt minimeringsprincip, således at kun identifikatoren for billedet fra referencedatabasen opbevares i logfilerne i stedet for at lagre referencebilledet. Logning af de biometriske datainput bør undgås, medmindre det er nødvendigt (f.eks. kun i tilfælde af overensstemmelse).

- ID for den bruger, der har anmodet om identifikations- eller verifikationsforsøget.

- alle personlige data, der gemmes i systemernes logfiler, er underlagt strenge formålsbegrænsninger (f.eks. revisioner) og bør ikke bruges til andre formål (f.eks. for stadig at kunne udføre genkendelse/verifikation, herunder et billede, der er blevet slettet fra referencedatabaserne). Der bør anvendes sikkerhedsforanstaltninger for at sikre logfilernes integritet, og automatiske overvågningssystemer til at opdage misbrug af logfiler anbefales stærkt. For så vidt angår logfilerne i referencedatabasen bør sikkerhedsforanstaltningerne svare til referencedatabasen i tilfælde af lagring af ansigtsbilleder. Der bør også implementeres automatiske processer for at sikre håndhævelse af dataopbevaringsperioden for logfilerne.

3.2.5.6 Artikel 4, stk. 4 – Ansvarlighed

102. Den dataansvarlige skal kunne påvise, at behandlingen er i overensstemmelse med principperne i artikel 4, stk. 1-3, jf. artikel 4, stk. 4, i retshåndhævelsesdirektivet. En systematisk og opdateret dokumentation af systemet (herunder opdateringer, opgraderinger og algoritmetræning), de tekniske og organisatoriske foranstaltninger (herunder overvågning af systemets ydeevne og potentiel menneskelig indgriben) og behandlingen af personoplysningerne er afgørende i denne henseende. For

[65] For yderligere oplysninger se EDPB's retningslinjer for databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

at påvise, at behandlingen er lovlig, er et særligt vigtigt element logning i henhold til artikel 25 i retshåndhævelsesdirektivet (jf. afsnit 3.2.5.5). Ansvarlighedsprincippet henviser ikke kun til systemet og behandlingen, men også til dokumentationen af proceduremæssige sikkerhedsforanstaltninger, såsom vurderinger af nødvendighed og forholdsmæssighed, konsekvensanalyser vedrørende databeskyttelse samt interne høringer (f.eks. ledelsens godkendelse af projektet eller interne afgørelser om pointværdier for konfidensscore) samt eksterne høringer (f.eks. databeskyttelsesmyndigheden). Bilag II indeholder en række elementer i denne henseende.

3.2.5.7 Artikel 47 – Effektiv undersøgelse

103. Effektive undersøgelsesbeføjelser fra de kompetente databeskyttelsesmyndigheders side er en af de vigtigste garantier for de grundlæggende rettigheder og frihedsrettigheder for de personer, der er berørt af brugen af ansigtsgenkendelsesteknologi. Samtidig er det en forudsætning for en effektiv udførelse af deres opgaver og udøvelse af deres beføjelser, at de enkelte datatilsynsmyndigheder råder over de nødvendige menneskelige, tekniske og finansielle ressourcer, lokaler og infrastrukturer[66]. Endnu vigtigere end antallet af tilgængelige medarbejdere er eksperternes færdigheder, som bør dække en meget bred vifte af spørgsmål – fra strafferetlig efterforskning og politisamarbejde til analyse af big data og kunstig intelligens. Derfor bør medlemsstaterne sikre, at tilsynsmyndighedernes ressourcer er passende og tilstrækkelige til, at de kan opfylde deres mandat til at beskytte de registreredes rettigheder, og nøje følge udviklingen i denne henseende[67].

4 KONKLUSION

104. Brugen af ansigtsgenkendelsesteknologier er uløseligt forbundet med behandling af betydelige mængder personoplysninger, herunder særlige kategorier af data. Ansigtet og mere generelt biometriske data er permanent og uigenkaldeligt knyttet til en persons identitet. Brug af ansigtsgenkendelse har derfor direkte eller indirekte indvirkning på en række grundlæggende rettigheder og frihedsrettigheder, der er nedfældet i EU's charter om grundlæggende rettigheder, og som kan gå videre end beskyttelse af privatlivets fred og databeskyttelse, såsom menneskelig værdighed, fri bevægelighed, forsamlingsfrihed m.fl. Dette er særlig relevant inden for retshåndhævelse og strafferet.

105. Databeskyttelsesrådet forstår behovet for, at retshåndhævende myndigheder får de bedst mulige redskaber til hurtigt at identificere gerningsmænd til terrorhandlinger og andre alvorlige strafbare handlinger. Sådanne værktøjer bør dog anvendes i nøje overensstemmelse med de gældende juridiske rammer og kun i tilfælde, hvor de opfylder kravene om nødvendighed og proportionalitet, som fastsat i artikel 52, stk. 1, i chartret. Og selv om moderne teknologier kan være en del af løsningen, er de på ingen måde en "mirakelløsning".

[66] Se Kommissionens meddelelse "Første rapport om anvendelsen og funktionen af direktiv (EU) 2016/680 om databeskyttelse på retshåndhævelsesområdet" (COM(2022) 364 final, punkt 3.4.1).
[67] Se Databeskyttelsesrådets bidrag til Europa-Kommissionens evaluering af direktivet om databeskyttelse på retshåndhævelsesområdet, jf. artikel 62, stk. 4, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

106. Der findes visse use cases for teknologier til ansigtsgenkendelse, som har uacceptabelt høje risici for enkeltpersoner og samfundet ("røde linjer"). Af disse grunde har Databeskyttelsesrådet og Den Europæiske Tilsynsførende for Databeskyttelse opfordret til et generelt forbud mod dem[68].

107. Især biometrisk fjernidentifikation af personer i offentligt tilgængelige rum udgør en høj risiko for indtrængen i enkeltpersoners privatliv og hører ikke hjemme i et demokratisk samfund, da det i sin natur indebærer masseovervågning. På samme måde mener Databeskyttelsesrådet, at AI-støttede ansigtsgenkendelsessystemer, der kategoriserer enkeltpersoner baseret på deres biometriske data i klynger efter etnicitet, køn samt politisk eller seksuel orientering, ikke er forenelige med chartret. Desuden er Databeskyttelsesrådet overbevist om, at brugen af ansigtsgenkendelse eller lignende teknologier til at udlede følelser hos en fysisk person stærkt må frarådes og bør forbydes, muligvis med få behørigt begrundede undtagelser. Desuden mener Databeskyttelsesrådet, at behandling af personoplysninger i en retshåndhævelsessammenhæng, der er baseret på en database, der er oprettet ved indsamling af personoplysninger i stor skala og på en vilkårlig måde, f.eks. ved "scraping" af fotografier og ansigtsbilleder, der er tilgængelige online, især dem, der er gjort tilgængelige via sociale netværk, som sådan ikke ville opfylde det strenge nødvendighedskrav, der er fastsat i EU-retten.

5 BILAG

Bilag I: Støtteskabelon

Bilag II: Praktisk vejledning for retshåndhævende myndigheder i håndtering af projekter med ansigtsgenkendelsesteknologi

Bilag III: Praktiske eksempler

[68] Se fælles udtalelse fra Databeskyttelsesrådet og Den Europæiske Tilsynsførende for Databeskyttelse 5/2021 om forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens).https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

BILAG I – SKABELON TIL BESKRIVELSE AF SCENARIER

(Med infobokse for de aspekter, der behandles i scenariet)

Beskrivelse af behandlingen:

- Beskrivelse af behandlingen, kontekst (kriminel relation), formål

Kilde til oplysninger:

- Typer af registrerede: ☐ alle borgere ☐ dømte ☐ mistænkte
  ☐ børn ☐ andre sårbare registrerede
- Billedkilde: ☐ offentligt tilgængelige steder ☐ internettet
  ☐ privat enhed ☐ andre enkeltpersoner ☐ andet

.....

- Forbindelse til kriminalitet: ☐ direkte tidsmæssig ☐ ikke direkte tidsmæssig
  ☐ direkte geografisk ☐ ikke direkte geografisk
  ☐ Ikke nødvendigt
- Indsamling af oplysninger: ☐ fjernovervågning ☐ i en kabine eller et kontrolleret miljø
- Kontekst – påvirker andre grundlæggende rettigheder:
  ☐ Nej
  Ja, dvs.: ☐ forsamlingsfrihed
  ☐ ytringsfrihed
  ☐ flere:.....
- Muligheder for yderligere kilder til information om den registrerede:
  ☐ ID-dokument ☐ brug af offentlig telefon ☐ køretøjs nummerplade
  ☐ andet .....

Referencedatabase (som de indsamlede oplysninger sammenlignes med):

- Specificitet: ☐ databaser til generelle formål☐ specifikke databaser relateret til kriminalitetsområdet
- Beskrivelse af, hvordan disse referencedatabaser blev udfyldt (og retsgrundlag)
- Ændring af formålet med databasen (f.eks. sikkerhed for privat ejendom var det primære mål):
  ☐ JA
  ☐ NEJ

Algoritme:

- Behandlingstype: ☐ 1:1-verifikation (autentifikation) ☐ 1:mange-identifikation
- Overvejelser om nøjagtighed
- Tekniske sikkerhedsforanstaltninger

Resultat:

- Indvirkning ☐ direkte (f.eks. den registrerede kan blive anholdt, afhørt, diskriminerende adfærd)

  ☐ ikke direkte (anvendes til statistiske modeller, ingen alvorlige retlige skridt mod registrerede)

- Automatiseret afgørelse: ☐ JA ☐ NEJ
- Opbevaringens varighed

Retlig analyse:

- Nødvendigheds- og proportionalitetsanalyse – forbrydelsens formål/alvor/antal personer, der ikke er involveret, men som er berørt af behandlingen
- Type af forudgående information til den registrerede: ☐ ved adgang til det specifikke område

  ☐ på den retshåndhævende myndigheds websted generelt

  ☐ på den retshåndhævende myndigheds websted for den specifikke behandling

  ☐ andet .....
- Gældende retlige rammer:

  ☐ Retshåndhævelsesdirektivet er for det meste kopieret til national ret

  ☐ Generisk national lovgivning for retshåndhævende myndigheders brug af biometriske data

  ☐ Specifik national lovgivning for denne behandling (ansigtsgenkendelse) for den pågældende kompetente myndighed

  ☐ Specifik national lovgivning for denne behandling (automatiseret afgørelse)

Konklusion:

Generelle overvejelser om, hvorvidt den beskrevne behandling sandsynligvis er forenelig med EU-retten (og nogle fingerpeg til juridiske forudsætninger)

BILAG II – PRAKTISK VEJLEDNING FOR RETSHÅNDHÆVENDE MYNDIGHEDER I HÅNDTERING AF PROJEKTER MED ANSIGTSGENKENDELSESTEKNOLOGI

Dette bilag giver yderligere praktisk vejledning til retshåndhævende myndigheder, der planlægger at igangsætte et projekt, der involverer ansigtsgenkendelsesteknologi. Det indeholder flere oplysninger om organisatoriske og tekniske foranstaltninger, der skal overvejes under gennemførelsen af projektet, og bør ikke betragtes som en udtømmende liste over skridt/foranstaltninger, der skal træffes. Det skal også ses i sammenhæng med Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger[69], gældende EU-/EØS-bestemmelser og Databeskyttelsesrådets retningslinjer vedrørende anvendelse af kunstig intelligens.

Dette bilag indeholder retningslinjer baseret på den antagelse, at retshåndhævende myndigheder vil indkøbe ansigtsgenkendelsesteknologi (som standardprodukter). Hvis de retshåndhævende myndigheder planlægger at udvikle (yderligere træne) ansigtsgenkendelsesteknologi, gælder der yderligere krav for udvælgelse af de nødvendige trænings-, validerings- og prøvningsdatasæt, der skal anvendes under udviklingen, og rollerne/foranstaltningerne for udviklingsmiljøet. På samme måde kan et standardprodukt kræve yderligere justeringer med hensyn til den tilsigtede anvendelse, og i så fald skal ovennævnte krav til udvælgelse af prøvnings-, validerings- og træningsdatasæt opfyldes.

Det at være medlem af samme retshåndhævende myndighed giver ikke i sig selv fuld adgang til biometriske data. Som med alle andre kategorier af personoplysninger kan biometriske data, der er indsamlet til et bestemt retshåndhævelsesformål under et specifikt retsgrundlag, ikke bruges uden et korrekt retsgrundlag til et andet retshåndhævelsesformål (artikel 4, stk. 2, i direktiv (EU) 2016/680 (retshåndhævelsesdirektivet)). Udvikling/træning af et værktøj til ansigtsgenkendelsesteknologi betragtes ligeledes som et andet formål, og det bør vurderes, om behandling af biometriske data for at måle ydeevne/træne teknologien for at undgå, at de registrerede påvirkes af lav ydeevne, er en nødvendig og forholdsmæssig foranstaltning under hensyntagen til det oprindelige formål med behandlingen.

1. ROLLER OG ANSVARSOMRÅDER

Når en retshåndhævende myndighed anvender ansigtsgenkendelsesteknologier til udførelse af sine opgaver, der er omfattet af retshåndhævelsesdirektivets anvendelsesområde (forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger osv., i henhold til artikel 3 i retshåndhævelsesdirektivet), kan den betragtes som dataansvarlig for ansigtsgenkendelsesteknologi. De retshåndhævende myndigheder består imidlertid af flere enheder/afdelinger, der kan være involveret i denne behandling, enten ved at definere processen for anvendelse af ansigtsgenkendelsesteknologi eller ved at anvende den i praksis. På grund af denne teknologis særlige egenskaber kan det være nødvendigt at inddrage forskellige enheder/afdelinger for at støtte målingerne af ydeevne eller for at træne teknologien.

[69] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

I et projekt, der involverer ansigtsgenkendelsesteknologi, er der flere interessenter[70] inden for de retshåndhævende myndigheder, som det kan være nødvendigt at inddrage:

- Topledelsen – skal godkende projektet efter at have afvejet risiciene i forhold til de potentielle fordele.
- Databeskyttelsesrådgiveren og/eller den retshåndhævende myndigheds juridiske afdeling – skal bistå med vurderingen af lovligheden af gennemførelsen af et bestemt projekt med ansigtsgenkendelsesteknologi; bistå med gennemførelsen af konsekvensanalysen vedrørende databeskyttelse; sikre overholdelse og udøvelse af de registreredes rettigheder.
- Procesejer – skal fungere som den specifikke enhed inden for den kompetente retshåndhævende myndighed, der skal udvikle projektet, beslutte detaljerne i det, herunder kravene til systemets ydeevne; beslutte den passende retfærdighedsmetrik; fastsætte konfidensscoren[71]; fastsætte acceptable tærskler for forudindtagethed; identificere de potentielle risici, som projektet med ansigtsgenkendelsesteknologi udgør for enkeltpersoners rettigheder og frihedsrettigheder (ved også at konsultere databeskyttelsesrådgiveren og IT AI og/eller Data science-afdelingen (se nedenfor)) og præsentere dem for den øverste ledelse. Procesejeren skal også konsultere referencedatabasens administrator, før der træffes beslutning om detaljerne i projektet med ansigtsgenkendelsesteknologi, for at forstå både formålet med referencedatabasen, men også dens tekniske detaljer. I tilfælde af træning af indkøbt ansigtsgenkendelsesteknologi er procesejeren også ansvarlig for udvælgelsen af træningsdatasættet. Som den enhed, der har til opgave at udarbejde og træffe beslutning om de nærmere detaljer om projektet, er procesejeren ansvarlig for at udføre konsekvensanalysen vedrørende databeskyttelse.
- IT AI og/eller Data science-afdeling – skal hjælpe med at udføre en konsekvensanalyse vedrørende databeskyttelse; forklare de tilgængelige metrikker til at måle systemets ydeevne, retfærdighed[72] og potentielle forudindtagethed; implementere teknologien og de tekniske sikkerhedsforanstaltninger for at forhindre uautoriseret adgang til de indsamlede data, cyberangreb osv. I tilfælde af træning af en indkøbt ansigtsgenkendelsesteknologi vil IT AI eller Data science-afdelingen skulle træne systemet baseret på det træningsdatasæt, som procesejeren har leveret. Denne afdeling vil også være ansvarlig for at etablere foranstaltninger til at afbøde de risici, som procesejerne har identificeret i fællesskab (f.eks. AI-specifikke risici som modelinferensangreb).
- Slutbrugere (f.eks. politimedarbejdere i marken eller i kriminaltekniske laboratorier) – skal foretage en sammenligning med databasen; foretage en kritisk gennemgang af resultaterne under hensyntagen til tidligere bevismateriale og give feedback til procesejeren for falske positive resultater og tegn på mulig forskelsbehandling.
- Referencedatabaseadministrator – den specifikke enhed i den kompetente retshåndhævende myndighed, der er ansvarlig for at akkumulere og forvalte referencedatabasen, dvs. den database, som billederne sammenlignes med, herunder sletning af ansigtsbilleder efter den fastsatte opbevaringsperiode. En sådan database kan oprettes specifikt til det påtænkte projekt med

[70] De følgende roller er vejledende for de forskellige interessenter og deres ansvar i forbindelse med et projekt med ansigtsgenkendelsesteknologi. Selv om den sprogbrug, der anvendes til at beskrive rollerne i dette bilag, ikke er kategorisk, er det op til den enkelte retshåndhævende myndighed at definere og tildele lignende roller i henhold til sin organisation. Det kan ske, at en enhed akkumulerer flere roller, f.eks. procesejer og referencedatabaseadministrator, eller procesejer og IT AI og/eller Data science-afdeling (når procesejerens enhed har al den nødvendige tekniske viden).

[71] Konfidensscoren er konfidensniveauet for forudsigelsen (matchningen) i form af en sandsynlighed. Ved at sammenligne to skabeloner er der f.eks. 90 % sikkerhed for, at disse tilhører den samme person. Konfidensscoren er ikke det samme som ansigtsgenkendelsesteknologiens ydeevne, men den påvirker ydeevnen. Jo højere konfidensgrænsen er, jo færre falske positive og jo flere falske negative er der i resultaterne fra ansigtsgenkendelsesteknologien.

[72] Retfærdighed kan defineres som fraværet af uretfærdig, ulovlig forskelsbehandling, som f.eks. forudindtagethed med hensyn til køn eller race.

ansigtsgenkendelsesteknologi eller kan eksistere i forvejen til kompatible formål. Referencedatabaseadministratoren er ansvarlig for at definere, hvornår og under hvilke omstændigheder ansigtsbilleder kan gemmes, samt for at fastsætte krav til dataopbevaring (i henhold til tid eller andre kriterier).

Da de fleste tilfælde af iværksættelse og anvendelse af ansigtsgenkendelsesteknologi indebærer en iboende høj risiko for registreredes rettigheder og frihedsrettigheder, bør tilsynsmyndigheden for databeskyttelse også inddrages i forbindelse med den forudgående høring, der kræves i henhold til retshåndhævelsesdirektivets artikel 28.

2. OPRETTELSE/INDEN INDKØB AF SYSTEMET FOR ANSIGTSGENKENDELSESTEKNOLOGI

Procesejeren i en retshåndhævende myndighed bør først have en klar forståelse af processen/processerne for ansigtsgenkendelsesteknologi (use case/s) og sikre, at der er et retsgrundlag for den tilsigtede anvendelse. På dette grundlag er følgende procesejerens ansvar:

- Formel beskrivelse af use casen. Det problem, der skal løses, og den måde, ansigtsgenkendelsesteknologien vil kunne løse det på, bør beskrives, såvel som de store linjer i den proces (opgave), hvor den vil blive anvendt. I denne henseende bør de retshåndhævende myndigheder som minimum dokumentere[73]:
  - de kategorier af personoplysninger, der registreres i processen
  - de mål og konkrete formål, som ansigtsgenkendelsesteknologi vil blive anvendt til, herunder de potentielle konsekvenser for den registrerede efter et match
  - hvornår og hvordan ansigtsbillederne vil blive indsamlet (herunder oplysninger om baggrunden for denne indsamling, f.eks. ved en lufthavnskontrol eller fra videoer fra sikkerhedskameraer uden for en butik, hvor der blev begået en forbrydelse, og de kategorier af registrerede, hvis biometriske data vil blive behandlet)
  - den database, som billeder vil blive sammenlignet med (referencedatabasen), samt oplysninger om, hvordan den blev oprettet, dens størrelse og kvaliteten af de biometriske data, den indeholder
  - de aktører i de retshåndhævende myndigheder, der vil få tilladelse til at anvende systemet med ansigtsgenkendelsesteknologi og følge det i forbindelse med retshåndhævelse (deres profiler og adgangsrettigheder skal defineres af procesejeren)
  - den planlagte opbevaringsperiode for de indlæste data, eller det tidspunkt, der bestemmer afslutningen af denne periode (såsom afslutning eller ophør af den straffesag i overensstemmelse med national retsplejelov, som de oprindeligt er blevet indsamlet til), samt enhver efterfølgende handling (sletning af disse data, anonymisering og brug til statistiske eller forskningsmæssige formål etc.)
  - implementering af logning og tilgængelighed af logfiler og optegnelser
  - ydeevneparametrene (f.eks. nøjagtighed, præcision, genkaldelse, F1-score) og deres acceptable minimumstærskler[74]

[73] Bilag I indeholder en liste over elementer, der hjælper den dataansvarlige med at beskrive en use case for ansigtsgenkendelsesteknologi.

[74] Der findes forskellige metoder til at evaluere ydeevnen af et system for ansigtsgenkendelsesteknologi. Hver af disse parametre giver et forskelligt billede af systemets resultater, og dets succes med at give et passende billede af, om systemet for ansigtsgenkendelsesteknologi fungerer godt eller ej, vil afhænge af use casen for ansigtsgenkendelsesteknologien. Hvis der fokuseres på at opnå en høj procentdel af korrekt matchning af et

- et skøn over, hvor mange mennesker der vil blive udsat for ansigtsgenkendelsesteknologi, i hvilken tidsperiode/ved hvilken lejlighed.

- Udførelse af en nødvendigheds- og proportionalitetsvurdering[75]. Det forhold, at denne teknologi eksisterer, bør ikke være drivkraften for at anvende den. Procesejeren skal først vurdere, om der findes et passende retsgrundlag for den påtænkte behandling. I den forbindelse skal databeskyttelsesrådgiveren og den juridiske tjeneste konsulteres. Drivkraften for at implementere ansigtsgenkendelsesteknologi bør være, at det er en nødvendig og proportionel løsning på et specifikt defineret problem for de retshåndhævende myndigheder. Dette skal vurderes i forhold til kriminalitetens formål/alvorlighed/antallet af personer, der ikke er involveret, men som er berørt af systemet med ansigtsgenkendelsesteknologi. I forbindelse med vurdering af lovligheden bør der som minimum tages hensyn til følgende: Retshåndhævelsesdirektivet[76], GDPR[7778], enhver eksisterende retlig ramme for kunstig intelligens[79] og alle ledsagende retningslinjer fra tilsynsmyndigheder for databeskyttelse (såsom Databeskyttelsesrådets retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger[80]). Disse EU-retsakter bør altid sammenlignes med de gældende nationale krav, især inden for strafferetsplejen. Proportionalitetsvurderingen bør identificere de registreredes grundlæggende rettigheder, der kan blive påvirket (ud over privatlivets fred og databeskyttelse). Den bør også beskrive og overveje eventuelle begrænsninger (eller manglende grænser), der i use casen er pålagt systemet med ansigtsgenkendelsesteknologi, f.eks. om systemet f.eks. skal køre kontinuerligt eller midlertidigt, og om det vil være begrænset til et geografisk område.
- Udførelse af en konsekvensanalyse vedrørende databeskyttelse[81]. Der bør gennemføres en konsekvensanalyse vedrørende databeskyttelse, da anvendelse af ansigtsgenkendelsesteknologi på retshåndhævelsesområdet kan resultere i en høj risiko for enkeltpersoners rettigheder og

ansigt, kan der anvendes parametre såsom præcision og genkaldelse. Disse parametre måler imidlertid ikke, hvor godt ansigtsgenkendelsesteknologien håndterer negative eksempler (hvor mange der fejlagtigt blev matchet af systemet). Procesejeren, støttet af IT AI og Data science-afdelingen, bør være i stand til at fastsætte kravene til ydeevne og udtrykke dem i den mest passende metrik i henhold til use casen for ansigtsgenkendelsesteknologien.

[75] Yderligere skridt til at tage hensyn til nødvendigheden kan overvejes med hensyn til at skræddersy og anvende systemet, og dermed kan beskrivelsen af use casen også ændres en smule i forbindelse med nødvendigheds- og proportionalitetsvurderingen.

[76] Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner.

[77] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

[78] I tilfælde, hvor et videnskabeligt projekt, der har til formål at undersøge brugen af ansigtsgenkendelsesteknologi, vil skulle behandle personoplysninger, men en sådan behandling ikke falder ind under artikel 4, stk. 3, i retshåndhævelsesdirektivet, vil GDPR generelt finde anvendelse (artikel 9, stk. 2, i retshåndhævelsesdirektivet). I tilfælde af pilotprojekter, der vil blive efterfulgt af retshåndhævelsesoperationer, vil retshåndhævelsesdirektivet stadig finde anvendelse.

[79] Der findes f.eks. et forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter, men forslaget er endnu ikke trådt i kraft som forordning.

[80] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

[81] Yderligere vejledning om konsekvensanalyser vedrørende databeskyttelse kan findes på: Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, WP 248 rev.01, tilgængelig på: https://ec.europa.eu/newsroom/article29/items/611236, og EDPS' Accountability on the ground toolkit, part II, tilgængelig på: https://edps.europa.eu/node/4582_en.

frihedsrettigheder[82]. Konsekvensanalysen vedrørende databeskyttelse bør navnlig indeholde: en generel beskrivelse af de planlagte behandlingsaktiviteter[83], en vurdering af risiciene for registreredes rettigheder og frihedsrettigheder[84], de foranstaltninger, der påtænkes for at imødegå disse risici, garantier, sikkerhedsforanstaltninger og mekanismer til at sikre beskyttelsen af personoplysninger og påvise overholdelse. Konsekvensanalysen vedrørende databeskyttelse er en løbende proces, så alle nye elementer i behandlingen bør tilføjes, og risikovurderingen bør ajourføres i hver fase af projektet.

- Indhentning af godkendelse fra den øverste ledelse ved at forklare risiciene for de registreredes rettigheder og frihedsrettigheder (fra use casen og teknologien) og de respektive risikohåndteringsplaner.

3. UNDER INDKØB OG INDEN IVÆRKSÆTTELSE AF ANSIGTSGENKENDELSESTEKNOLOGIEN

- Fastlæggelse af kriterierne for valg af ansigtsgenkendelsesteknologi (algoritme). Procesejeren skal beslutte kriterierne for valg af en algoritme med hjælp fra IT AI og/eller Data science-afdelingen. I praksis vil disse omfatte retfærdigheds- og ydeevneparametre, der er fastsat i beskrivelsen af brugstilfældet. Sådanne kriterier bør også omfatte oplysninger vedrørende data, som algoritmen er blevet trænet sammen med. Trænings-, afprøvnings- og valideringssættet skal i tilstrækkelig grad omfatte stikprøver af alle karakteristika hos de registrerede, der skal være omfattet af ansigtsgenkendelsesteknologien (overvej f.eks. alder, køn og race) for at reducere forudindtagethed. Leverandøren af ansigtsgenkendelsesteknologien bør fremlægge oplysninger og parametre om trænings-, test- og valideringsdatasættene for ansigtsgenkendelsesteknologien og beskrive de foranstaltninger, der er truffet for at måle og afbøde potentiel ulovlig forskelsbehandling og forudindtagethed. Procesejeren skal, hvor det er muligt, kontrollere, om der eksisterede et retsgrundlag for udbyderen til at bruge dette datasæt til træning af algoritmerne (baseret på oplysninger, som udbyderen stiller til rådighed). Procesejeren bør også sikre, at udbyderen af ansigtsgenkendelsesteknologien anvender sikkerhedsstandarder vedrørende biometriske data, såsom ISO/IEC 24745, som giver vejledning i beskyttelse af biometriske oplysninger i henhold til forskellige krav til fortrolighed, integritet og fornyelighed/tilbagekaldelsesmulighed under lagring og overførsel samt krav og retningslinjer for sikker forvaltning og behandling af biometriske oplysninger, der er i overensstemmelse med privatlivets fred.

- Gentræning af algoritmen (om nødvendigt). Procesejeren bør sikre, at finjustering af systemet for ansigtsgenkendelsesteknologi for at opnå højere nøjagtighed, før det bruges, også er en del af de indkøbte tjenester. Hvis det er nødvendigt med yderligere træning af det erhvervede system for ansigtsgenkendelsesteknologi for at opfylde nøjagtighedsparametrene, skal procesejeren, bortset

[82] Ansigtsgenkendelsesteknologi kan, afhængigt af use casen, være omfattet af følgende kriterier, der udløser højrisikobehandling (fra retningslinjerne for konsekvensanalyse vedrørende databeskyttelse, WP 248 rev.01): Systematisk overvågning, databehandling i stor skala, matchning eller kombination af datasæt, innovativ brug eller anvendelse af nye teknologiske eller organisatoriske løsninger.

[83] Beskrivelsen af behandlingen samt nødvendigheds- og proportionalitetsvurderingen – som allerede beskrevet i ovenstående trin – indgår også i konsekvensanalysen vedrørende databeskyttelse, bortset fra risikovurderingen. Om nødvendigt kan der gives en mere detaljeret beskrivelse af persondatastrømmene i konsekvensanalysen.

[84] Analysen af risiciene for de registrerede bør omfatte risici i forbindelse med stedet for de ansigtsbilleder, der skal sammenlignes (lokalt/fjernt), risici i forbindelse med databehandlere/underdatabehandlere samt risici, der er specifikke for maskinlæring, når dette anvendes (f.eks. dataforgiftning, kontradiktoriske eksempler).

fra at træffe beslutning om gentræning, med hjælp fra IT AI og/eller Data science-afdelingen beslutte, hvilket tilstrækkeligt og repræsentativt datasæt der skal anvendes, og kontrollere lovligheden af denne anvendelse af dataene.

- Fastsættelse af passende sikkerhedsforanstaltninger for at behandle risici i forbindelse med sikkerhed, forudindtagethed og lav ydeevne. Dette omfatter etablering af en proces til overvågning af ansigtsgenkendelsesteknologien, når den er i brug (logning og feedback med henblik på at sikre, at resultaterne er nøjagtige og retfærdige). Sørg desuden for, at de risici, der er specifikke for nogle systemer for maskinlæring og ansigtsgenkendelsesteknologi (f.eks. dataforgiftning, kontradiktoriske eksempler, modelinversion, white-box-inferens), identificeres, måles og afbødes. Procesejeren bør også fastsætte passende sikkerhedsforanstaltninger for at sikre, at kravene til opbevaring af biometriske data, der indgår i gentræningsdatasættet, overholdes.
- Dokumentation af systemet for ansigtsgenkendelsesteknologi. Dette bør omfatte en generel beskrivelse af systemet, en detaljeret beskrivelse af elementerne i det og af processen for dets etablering, detaljerede oplysninger om overvågning, funktion og kontrol af systemet og en detaljeret beskrivelse af dets risici og afbødende foranstaltninger. Elementerne i denne dokumentation omfatter hovedelementerne i systembeskrivelsen for ansigtsgenkendelsesteknologien fra tidligere faser (se ovenfor), men de udvides med oplysninger om overvågning af ydeevne og anvendelse af ændringer i systemet, herunder eventuelle versionsopdateringer og/eller gentræning.
- Oprettelse af brugermanualer, der forklarer teknologien og de pågældende use cases. Disse skal forklare alle scenarier og forudsætninger, under hvilke der vil blive gjort brug af ansigtsgenkendelsesteknologi på en klar måde.
- Uddannelse af slutbrugerne i, hvordan de bruger teknologien. Sådanne kurser skal forklare teknologiens kapacitet og begrænsninger, så brugerne kan forstå, under hvilke omstændigheder det er nødvendigt at anvende den, og i hvilke tilfælde den kan være unøjagtig. En sådan uddannelse vil også bidrage til at mindske risici i forbindelse med manglende kontrol/kritisk gennemgang af algoritmeresultatet.
- Høring af tilsynsmyndigheden for databeskyttelse i henhold til retshåndhævelsesdirektivets artikel 28, stk. 1, litra b). Tilvejebringe information i henhold til artikel 13 i retshåndhævelsesdirektivet for at informere de registrerede om behandlingen og deres rettigheder. Denne information skal henvende sig til de registrerede i et passende sprog, så de er i stand til at forstå behandlingen, og forklare de grundlæggende elementer i teknologien, herunder nøjagtighedsprocenter, træningsdatasæt og foranstaltninger, der er truffet for at undgå forskelsbehandling og lav nøjagtighed i algoritmen.

4. ANBEFALINGER EFTER IVÆRKSÆTTELSE AF ANSIGTSGENKENDELSESTEKNOLOGIEN

- Sikring af menneskelig indgriben og tilsyn med resultaterne. Træf aldrig nogen foranstaltning vedrørende en person udelukkende baseret på resultatet af ansigtsgenkendelsesteknologi (det ville indebære en overtrædelse af artikel 11 i retshåndhævelsesdirektivet – automatiske individuelle afgørelser med retsvirkninger eller andre lignende virkninger for den registrerede). Sørg for, at en retshåndhævelsesmedarbejder gennemgår resultaterne af ansigtsgenkendelsesteknologien. Sørg ligeledes for, at brugere i de retshåndhævende myndigheder undgår automatiseringsbias ved at undersøge modstridende oplysninger og kritisk udfordre teknologiens resultater. Til dette formål er det vigtigt med løbende uddannelse og oplysning til slutbrugerne, men den øverste ledelse bør sikre, at der er tilstrækkelige menneskelige ressourcer til at føre effektivt tilsyn. Det indebærer, at den enkelte medarbejder får

tid nok til kritisk at udfordre teknologiens resultater. Registrer, mål og vurder, i hvilket omfang det menneskelige tilsyn ændrer den oprindelige afgørelse fra ansigtsgenkendelsesteknologien.

- Overvågning og håndtering af afvigelser i modellen for ansigtsgenkendelsesteknologi (forringelse af ydeevne), når modellen er i produktion.
- Fastlæggelse af en proces til at revurdere risiciene og sikkerhedsforanstaltningerne regelmæssigt, og hver gang teknologien eller use casen ændrer sig.
- Dokumentation af enhver ændring af systemet i hele dets livscyklus (f.eks. opgraderinger og gentræning).
- Fastsættelse af en proces og de tilhørende tekniske muligheder for at behandle anmodninger om adgang fra de registrerede. Den tekniske kapacitet til at udtrække data, hvis der er behov for at give dem til de registrerede, skal være på plads, før der kommer en anmodning.
- Iværksættelse af procedurer i tilfælde af brud på datasikkerheden. Hvis der opstår et brud på persondatasikkerheden, der involverer biometriske data, vil risiciene sandsynligvis være store. I dette tilfælde skal alle involverede brugere være opmærksomme på de relevante procedurer, der skal følges, databeskyttelsesrådgiveren skal straks informeres, og de registrerede skal informeres.

BILAG III – PRAKTISKE EKSEMPLER

Der er mange forskellige praktiske indstillinger og formål med at bruge ansigtsgenkendelse, f.eks. i kontrollerede miljøer som ved grænseovergange, krydstjek med data fra politidatabaser eller fra persondata, der tydeligvis er offentliggjort af den registrerede, live kamera-feeds (live ansigtsgenkendelse) osv. Som følge heraf varierer risiciene for beskyttelsen af personoplysninger og andre grundlæggende rettigheder og frihedsrettigheder betydeligt i de forskellige use cases. For at lette nødvendigheds- og proportionalitetsvurderingen, som bør gå forud for afgørelsen om en eventuel indførelse af ansigtsgenkendelse, indeholder disse retningslinjer en ikke-udtømmende liste over mulige anvendelser af ansigtsgenkendelsesteknologi på retshåndhævelsesområdet.

De scenarier, der præsenteres og vurderes, er baseret på **hypotetiske** situationer og har til formål at illustrere visse konkrete anvendelser af ansigtsgenkendelsesteknologi og give hjælp til overvejelser fra sag til sag samt at sætte en overordnet ramme. De forsøger ikke at være udtømmende og berører ikke eventuelle igangværende eller fremtidige procedurer, der iværksættes af en national tilsynsmyndighed, med hensyn til udformning, forsøg eller gennemførelse af teknologier til ansigtsgenkendelse. Præsentationen af disse scenarier skal kun tjene det formål at eksemplificere den vejledning til politiske beslutningstagere, lovgivere og retshåndhævende myndigheder, der allerede er givet i dette dokument, til udformning og opstilling af konturerne for en iværksættelse af ansigtsgenkendelsesteknologi, og er medtaget i den hensigt at sikre fuld overensstemmelse med EU's regelværk inden for beskyttelse af persondata. I denne forbindelse skal det erindres, at selv i tilsyneladende ens situationer med brug af ansigtsgenkendelsesteknologi kan tilstedeværelse eller fravær af nogle elementer føre til et andet resultat af nødvendigheds- og proportionalitetsvurderingen.

1 SCENARIE 1

1.1. Beskrivelse

Et automatiseret grænsekontrolsystem, der muliggør automatiseret grænsepassage ved at autentificere det biometriske billede, der er gemt i det elektroniske rejsedokument for EU-borgere og andre rejsende, der passerer grænsepassagen, og fastslå, at personen er den retmæssige indehaver af dokumentet.

En sådan verificering/autentificering involverer kun 1:1-ansigtsgenkendelse og udføres i kontrollerede omgivelser (f.eks. ved lufthavnes elektroniske paskontroller). De biometriske data om den rejsende, der passerer grænsepassagen, registreres, når vedkommende udtrykkeligt opfordres til at se mod kameraet i den elektroniske paskontrol, og sammenlignes med oplysningerne i det forelagte dokument (pas, identitetskort osv.), som er udstedt i henhold til specifikke tekniske krav.

Selv om behandlingen i sådanne tilfælde i princippet falder uden for retshåndhævelsesdirektivets anvendelsesområde, kan resultatet af verifikationen også bruges til at matche (alfanumeriske) data om personen med retshåndhævende databaser som en del af grænsekontrollen og kan således medføre handlinger med betydelig retsvirkning for den registrerede, f.eks. anholdelse i henhold til en efterlysning i SIS. Under særlige omstændigheder kan de biometriske data også bruges til at søge efter matches i retshåndhævende databaser (i så fald vil der blive udført 1:mange-identifikation på dette trin).

Resultatet af behandlingen af biometriske billeder har direkte indvirkning på den registrerede: Kun i tilfælde af en vellykket verifikation giver det mulighed for at passere grænsepassagen. I tilfælde af

mislykket identifikation er grænsevagterne nødt til at udføre endnu et tjek for at sikre, at den registrerede ikke er den person, der er afbildet i identifikationsdokumentet.

Hvis en SIS- eller national efterlysning konstateres, skal grænsevagterne foretage endnu en verifikation og de nødvendige yderligere kontroller og derefter træffe de nødvendige foranstaltninger, f.eks. anholde personen og informere de berørte myndigheder.

Kilde til oplysninger:

- Typer af registrerede: ☒ alle personer, der passerer grænserne
- Kilde til billede: ☒ andet (ID-dokument)
- Forbindelse til kriminalitet: ☒ ikke nødvendigt
- Metode til indsamling af oplysninger: ☒ i en kabine eller et kontrolleret miljø.
- Kontekst – påvirker andre grundlæggende rettigheder: Ja, dvs.: ☒ ret til fri bevægelighed
  ☒ ret til asyl

Referencedatabase (som de indsamlede oplysninger sammenlignes med):

- Specificitet: ☒ specifikke databaser relateret til grænsekontrol.

Algoritme:

- Verifikationstype: ☒ 1:1-verifikation (autentifikation)

Resultat:

- Indvirkning ☒ direkte (den registrerede tillades eller nægtes indrejse)
- Automatiseret afgørelse: ☒ ja

1.2. Gældende retlige rammer

Siden 2004 skal pas og andre rejsedokumenter, der udstedes af medlemsstaterne, i henhold til Rådets forordning (EF) nr. 2252/2004[85] indeholde et biometrisk ansigtsbillede, som lagres i en elektronisk chip, der er indbygget i dokumentet.

Schengengrænsekodeksen (SBC)[86] fastlægger kravene til grænsekontrol af personer ved de ydre grænser. For EU-borgere og andre personer, der har ret til fri bevægelighed i henhold til EU-retten, bør minimumskontrollen bestå i en kontrol af deres rejsedokumenter, om nødvendigt ved hjælp af tekniske hjælpemidler. Schengengrænsekodeksen er efterfølgende blevet ændret med forordning (EU) 2017/2225[87], som bl.a. indførte definitioner for "elektronisk paskontrol", "automatisk grænsekontrol" og "selvbetjeningssystem" samt muligheden for at behandle biometriske data med henblik på grænsekontrol.

Det kan derfor antages, at der er et klart og forudsigeligt retsgrundlag, som tillader denne form for behandling af personoplysninger. Desuden er den juridiske ramme vedtaget på EU-plan og gælder direkte for medlemsstaterne.

1.3. Nødvendighed og proportionalitet – forbrydelsens formål/alvorlighed

Verifikation af EU-borgeres identitet i en automatisk grænsekontrol ved hjælp af deres biometriske billede er et element i grænsekontrollen ved EU's ydre grænser. Den er derfor direkte knyttet til grænsesikkerhed og tjener et mål af almen interesse, der er anerkendt af Unionen. Derudover bidrager

[85] Rådets forordning (EF) Nr. 2252/2004 af 13. december 2004 om standarder for sikkerhedselementer og biometriske identifikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder.
[86] Europa-Parlamentets og Rådets forordning (EU) nr. 2016/399 af 9. marts 2016 om en EU-kodeks for personers grænsepassage (Schengengrænsekodeks).
[87] Europa-Parlamentets og Rådets forordning (EU) 2017/2225 af 30. november 2017 om ændring af forordning (EU) 2016/399, for så vidt angår brugen af ind- og udrejsesystemet.

den automatiske grænsekontrol til at fremskynde behandlingen af passagerer og mindske risikoen for menneskelige fejl. Desuden er omfanget, udstrækningen og intensiteten af indgrebet i dette scenarie langt mere begrænset sammenlignet med andre former for ansigtsgenkendelse. Ikke desto mindre skaber behandlingen af biometriske data yderligere risici for de registrerede, som den kompetente myndighed, der iværksætter og anvender ansigtsgenkendelsesteknologien, skal håndtere og afbøde behørigt.

1.4. Konklusion

Kontrol af EU-borgernes identitet i forbindelse med automatisk grænsekontrol er en nødvendig og forholdsmæssig foranstaltning, så længe de fornødne garantier er på plads, navnlig anvendelsen af principperne om formålsbegrænsning, datakvalitet, gennemsigtighed og et højt sikkerhedsniveau.

2 SCENARIE 2

2.1. Beskrivelse

Et system til identifikation af ofre for børnebortførelser iværksættes af de retshåndhævende myndigheder. En autoriseret politimedarbejder kan foretage en sammenligning af de biometriske data for et barn, der mistænkes for at være bortført, med en database over ofre for børnebortførelser under strenge betingelser og med det ene formål at identificere mindreårige, der kan svare til beskrivelsen af det forsvundne barn, for hvem der er indledt en efterforskning og udsendt en efterlysning.

Den behandling, der er tale om, vil være sammenligningen af ansigtet eller billedet af en person, der måske svarer til beskrivelsen af et forsvundet barn, med de billeder, der er gemt i databasen. En sådan behandling vil finde sted i specifikke tilfælde og ikke på et systematisk grundlag.

Den database, som sammenligningen vil blive anvendt på, indeholder billeder af forsvundne børn, for hvilke der er indberettet mistanke om bortførelse eller en trussel mod barnets liv eller dets fysiske integritet, hvor en strafferetlig efterforskning under en retslig myndighed er indledt og hvor en efterlysning vedrørende bortførelse af børn er udsendt. Oplysningerne indsamles inden for rammerne af de procedurer, der er fastlagt af den kompetente retshåndhævende myndighed, dvs. politimedarbejdere, der er bemyndiget til at udføre kriminalpolitimissioner. De kategorier af personoplysninger, der registreres, er:

- identitet, kaldenavn, alias, slægtskab, nationalitet, adresser, e-mailadresser, telefonnumre
- fødselsdato og -sted
- oplysninger om forældre
- fotografier med tekniske funktioner, der gør det muligt at anvende en anordning til ansigtsgenkendelse og andre fotografier.

Sammenligningsresultaterne skal endvidere gennemgås og verificeres af en bemyndiget medarbejder for at underbygge tidligere dokumentation med resultatet af sammenligningen og udelukke eventuelle falske positive resultater.

Billeder af børn og personoplysninger må kun opbevares, så længe efterlysningen opretholdes, og skal slettes umiddelbart efter afslutning eller ophør af straffesagen i overensstemmelse med de nationale procedurer, som er baggrunden for indlæsningen i databasen.

Selv om opbevaringsperioden for biometriske data i databasen kan forventes at være relativt lang og er defineret i henhold til national lovgivning, udgør udøvelsen af registreredes rettigheder og navnlig retten til berigtigelse og sletning en yderligere garanti for at begrænse indgrebet i de berørte registreredes ret til beskyttelse af personoplysninger.

Kilde til oplysninger:

- Typer af registrerede: ☒ børn
- Kilde til billede ☒ andet: ikke foruddefineret, mistænkt offer for børnebortførelse
- Forbindelse til kriminalitet: ☒ ikke direkte tidsmæssig ☒ ikke direkte geografisk
- Metode til indsamling af oplysninger: ☒ i en kabine eller et kontrolleret miljø.
- Kontekst: påvirker andre grundlæggende rettigheder ☒ ja, dvs.: ☒ forskellige

Referencedatabase (som de indsamlede oplysninger sammenlignes med):

- Specificitet ☒ specifik database

Algoritme:

- Verifikationstype: ☒ 1:mange-identifikation

Resultat:

- Indvirkning: ☒ direkte
- Automatiseret afgørelse: ☒ NEJ, obligatorisk gennemgang foretaget af en bemyndiget medarbejder

Retlig analyse:

- Gældende retlig ramme: ☒ specifik national lovgivning for denne behandling (ansigtsgenkendelse)

2.2. Gældende retlige rammer

Den nationale lovgivning indeholder en særlig retlig ramme for oprettelse af databasen, der fastlægger formålet med behandlingen samt kriterierne for, hvornår databasen skal udfyldes, tilgås og anvendes. De lovgivningsmæssige foranstaltninger, der er nødvendige for dens gennemførelse, indeholder også bestemmelser om fastlæggelse af en opbevaringsperiode samt henvisning til de gældende principper om integritet og fortrolighed. De lovgivningsmæssige foranstaltninger indeholder også bestemmelser om de nærmere bestemmelser for underretning af den registrerede og i dette tilfælde indehaveren/indehaverne af forældreansvaret samt udøvelsen af den registreredes rettigheder og en eventuel begrænsning, hvis det er relevant. Under forberedelsen af forslaget til den respektive lovforanstaltning skulle den nationale tilsynsmyndighed konsulteres.

2.3. Nødvendighed og proportionalitet – forbrydelsens formål/alvor/antal personer, der ikke er involveret, men som er berørt af behandlingen

Betingelser og sikkerhedsforanstaltninger for behandling

Ansigtsgenkendelsessammenligningen kan kun udføres af en autoriseret medarbejder som en sidste udvej, hvor der ikke er andre mindre indgribende midler til rådighed, og hvor det er strengt nødvendigt, f.eks. i tilfælde af tvivl om ægtheden af en rejsende mindreårigs identitetsdokument og/eller efter at have gennemgået tidligere beviser og indsamlet materiale, der indikerer en mulig overensstemmelse med beskrivelsen af et forsvundet barn, for hvilket der udføres en strafferetlig efterforskning.

En yderligere sikkerhedsforanstaltning er den obligatoriske gennemgang og verificering af ansigtsgenkendelsessammenligningen af en autoriseret medarbejder for at bekræfte tidligere beviser med resultatet af sammenligningen og udelukke eventuelle falske positive resultater.

Det forfulgte formål

Oprettelsen af databasen tjener vigtige formål af almen interesse, navnlig forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger eller fuldbyrdelse af strafferetlige sanktioner og beskyttelse af andres rettigheder og frihedsrettigheder. Oprettelsen af databasen og den planlagte behandling ser ud til at bidrage til identifikationen af børn, der er ofre for bortførelser, og kan derfor betragtes som en foranstaltning, der er egnet til at støtte det legitime mål om at efterforske og retsforfølge sådanne forbrydelser.

Databasens formål og indhold

Formålet med behandlingen er klart defineret ved lov, og databasen må kun bruges til at identificere forsvundne børn, for hvilke der er indberettet en mistanke om bortførelse, indledt en strafferetlig efterforskning under tilsyn af en retslig myndighed, og udsendt en efterlysning om bortførelse. De betingelser, der er fastsat ved lov for indholdet af databasen, har til formål nøje at begrænse antallet af registrerede og personoplysninger, der skal indgå i databasen. Indehaveren af forældremyndigheden over barnet skal informeres om den behandling, der foretages, og betingelserne for udøvelsen af barnets rettigheder i forbindelse med den biometriske behandling, der påtænkes med henblik på identifikation, eller de personoplysninger om barnet, der opbevares i databasen.

2.4. Konklusion

I betragtning af nødvendigheden og proportionaliteten af den påtænkte behandling samt hensynet til barnets tarv ved udførelsen af en sådan behandling af personoplysninger, og forudsat at der er tilstrækkelige garantier på plads til især at sikre udøvelsen af registreredes rettigheder – navnlig under hensyntagen til det faktum, at det er børns data der behandles, kan en sådan anvendelse af ansigtsgenkendelsesbehandling anses for sandsynligvis at være forenelig med EU-lovgivningen.

I betragtning af typen af behandling og den anvendte teknologi, som indebærer en høj risiko for de berørte registreredes rettigheder og frihedsrettigheder, mener Databeskyttelsesrådet desuden, at udarbejdelse af et forslag til en lovgivningsmæssig foranstaltning, der skal vedtages af et nationalt parlament, eller af en lovgivningsmæssig foranstaltning, der har hjemmel i en sådan lovgivningsmæssig foranstaltning, som vedrører den påtænkte behandling, bør omfatte en forudgående høring af tilsynsmyndigheden for at sikre sammenhæng og overholdelse af den gældende retlige ramme, jf. artikel 28, stk. 2, i retshåndhævelsesdirektivet.

3 SCENARIE 3

3.1. Beskrivelse

I forbindelse med politiets indsats under optøjer og efterfølgende efterforskninger er en række personer blevet identificeret som mistænkte, f.eks. gennem tidligere efterforskninger ved hjælp af overvågningskameraer eller vidner. Billeder af disse mistænkte sammenlignes med billeder af personer, der er optaget med overvågningskameraer eller mobile enheder på et gerningssted eller i de omkringliggende områder.

For at indhente mere detaljeret dokumentation om personer, der mistænkes for at have deltaget i optøjer i forbindelse med en demonstration, opretter politiet en database bestående af billedmateriale med løs geografisk og tidsmæssig forbindelse til optøjerne. Databasen omfatter private optagelser, som borgere har uploadet til politiet, materiale fra offentlige transportmidlers overvågningskameraer, politiets eget videoovervågningsmateriale og materiale offentliggjort af medierne uden nogen specifik begrænsning eller sikkerhedsforanstaltning. Indhold med alvorlig kriminel adfærd er ikke en forudsætning for de filer, der indgår i databasen. Derfor er billeder af personer, der ikke var involveret i optøjerne – en betydelig procentdel af lokalbefolkningen, som tilfældigvis kom forbi, da demonstrationen fandt sted, eller som deltog i demonstrationen, men ikke i optøjerne – opbevaret i databasen. Basen indeholder tusindvis af video- og billedfiler.

Ved hjælp af en ansigtsgenkendelsessoftware tildeles alle ansigter, der optræder i disse filer, unikke ansigts-ID'er. Ansigterne på de enkelte mistænkte sammenlignes derefter automatisk med disse ansigts-ID'er. Databasen, der består af alle de biometriske skabeloner i de tusindvis af video- og billedfiler, opbevares, indtil alle mulige efterforskninger er afsluttet. Positive match behandles af de ansvarlige medarbejdere, som derefter træffer beslutning om yderligere tiltag. Dette kan omfatte at henføre den fil, der findes i databasen, til den pågældende persons straffesag, eller yderligere foranstaltninger, såsom afhøring eller anholdelse af den pågældende person.

En national lov indeholder en generisk bestemmelse, hvorefter behandling af biometriske data med det formål entydigt at identificere en fysisk person er tilladt, hvis det er strengt nødvendigt og underlagt passende garantier for den berørte persons rettigheder og frihedsrettigheder.

Kilde til oplysninger:

- Typer af registrerede: ☒ alle personer
- Kilde til billede: ☒ offentligt tilgængelige steder ☒ privat enhed ☒ andre personer ☒ andet: medier
- Tilknytning til kriminalitet: ☒ ikke nødvendigvis direkte geografisk eller tidsmæssig forbindelse
- Metode til indsamling af oplysninger: ☒ fjernovervågning
- Kontekst – påvirker andre grundlæggende rettigheder: Ja, dvs.: ☒ kontekst med forsamlingsfrihed
- Tilgængelige yderligere kilder til information om den registrerede:
  ☒ andet: ikke udelukket (f.eks. brug af hæveautomater eller besøg i butikker), da der ikke kan udøves kontrol over indhold af billederne.

Referencedatabase (som de indsamlede oplysninger sammenlignes med):

- Specificitet: ☒ specifikke databaser relateret til kriminalitetsområdet.

Algoritme:

- Behandlingstype: ☒ 1:mange-identifikation

Resultat:

- Indvirkning: ☒ direkte (f.eks. kan den registrerede blive anholdt, afhørt)
- Automatiseret afgørelse: ☒ NEJ
- Opbevaringsvarighed: indtil alle mulige undersøgelser er afsluttet

Retlig analyse:

- Type af forudgående information til den registrerede: ☒ på retshåndhævende myndigheders hjemmeside generelt

- Gældende retlig ramme: ☒ Retshåndhævelsesdirektivet er generelt kopieret til national lovgivning ☒ Generisk national lovgivning for retshåndhævende myndigheders brug af biometriske data

3.2. Gældende retlige rammer

Som præciseret ovenfor er retsgrundlag, der blot gentager den generelle bestemmelse i artikel 10 i retshåndhævelsesdirektivet, ikke tilstrækkeligt klare i deres ordlyd til at give enkeltpersoner en passende indikation af de betingelser og omstændigheder, hvorunder de retshåndhævende myndigheder har beføjelse til at anvende optagelser fra overvågningskameraer på offentlige steder til at oprette en biometrisk skabelon af deres ansigt og sammenligne den med politiets databaser, andre tilgængelige overvågningskameraoptagelser eller private optagelser osv. Den retlige ramme, der er fastlagt i dette scenarie, opfylder derfor ikke minimumskravene til at tjene som retsgrundlag.

3.3. Nødvendighed og proportionalitet

I dette eksempel giver behandlingen anledning til forskellige betænkeligheder under nødvendigheds- og proportionalitetsprincippet af flere grunde:

Personer mistænkes ikke for at have begået en alvorlig forbrydelse. Det er ikke en forudsætning for anvendelse af filerne i databasen, der indeholder billedmaterialet, at der vises grov kriminel adfærd. En direkte tidsmæssig og geografisk forbindelse til forbrydelsen er heller ikke en forudsætning for brugen af filerne i databasen. Dette resulterer i, at billeder af en betydelig procentdel af den lokale befolkning lagres i en biometrisk database i en periode på potentielt flere år, indtil alle undersøgelser er afsluttet.

Gerningsstedsdatabasen er ikke begrænset til billeder, der opfylder proportionalitetskravene, hvilket fører til en ubegrænset mængde billeder, der kan sammenlignes. Dette er i strid med princippet om dataminimering. En mindre mængde billeder ville også gøre det muligt at overveje ikke-algoritmiske og mindre indgribende metoder, f.eks. supergenkendere[88].

Da eksemplet er taget fra en demonstration, er det også sandsynligt, at billederne afslører politiske holdninger hos deltagerne i demonstrationen, hvilket er den anden særlige kategori af data, der muligvis påvirkes i dette scenarie. I dette scenarie er det uklart, hvordan indsamlingen af disse data kan forebygges, og med hvilke sikkerhedsforanstaltninger. Når de registrerede får at vide, at deres deltagelse i en demonstration har resulteret i, at de er blevet registreret i en biometrisk politidatabase, kan det desuden have en alvorlig afskrækkende virkning på deres fremtidige udøvelse af deres ret til at forsamles.

De biometriske skabeloner i databasen kan også sammenlignes med hinanden. Det gør det muligt for politiet ikke bare at lede efter en bestemt person i alt deres materiale, men også at genskabe en persons adfærdsmønster over en periode på flere dage. Der kan også indsamles yderligere oplysninger om personerne, såsom sociale kontakter og politisk engagement.

Indgrebet forstærkes yderligere af det faktum, at dataene behandles uden de registreredes viden.

[88] Dvs. mennesker med en ekstraordinær evne til at genkende ansigter. Jf. også: Face Recognition by Metropolitan Police Super-Recognisers (ansigtsgenkendelse med supergenkendere i Londons politi), 2016. februar 26, DOI: 10.1371/journal.pone.0150036 https://pubmed.ncbi.nlm.nih.gov/26918457/.

Når man tænker på, at personer hele tiden optager fotografier og videoer, og at selv den allestedsnærværende brug af overvågningskameraer kan analyseres biometrisk, kan det føre til alvorlige afskrækkende virkninger.

Den omfattende brug af private fotografier og videoer, herunder potentielt misbrug i form af angiveri, er et andet punkt, der giver anledning til bekymring. Da misbrug i form af angiveri også er en risiko, der er forbundet med straffesager generelt, er risikoen betydeligt højere, når mængden af behandlet data og antallet af involverede personer kan skaleres, da folk også kan uploade materiale, der vedrører en bestemt person eller gruppe af personer, som de ikke bryder sig om. Politiets anmodninger om at uploade fotografier og videoer fører muligvis til meget lave tærskler for, at folk leverer materiale, især da det kan være muligt at gøre det anonymt eller i det mindste uden at skulle møde op og identificere sig selv på en politistation.

3.4. Konklusion

I eksemplet er der ingen specifik bestemmelse, der kunne tjene som retsgrundlag. Men selv hvis der var et tilstrækkeligt retsgrundlag, ville kravene om nødvendighed og proportionalitet ikke være opfyldt, hvilket ville resultere i et uforholdsmæssigt stort indgreb i den registreredes ret til respekt for privatliv og beskyttelse af personoplysninger i henhold til chartret.

4 SCENARIE 4

4.1. Beskrivelse

Politiet iværksætter en metode til at identificere mistænkte, der begår en alvorlig forbrydelse, som er optaget på overvågningskameraer, ved hjælp af ansigtsgenkendelsesteknologi, der anvendes med tilbagevirkende kraft En medarbejder udvælger manuelt billede(r) af mistænkte i det videomateriale, der er indsamlet fra gerningsstedet eller andre steder i forbindelse med en indledende efterforskning, og sender dem til den kriminaltekniske afdeling. Den kriminaltekniske afdeling bruger ansigtsgenkendelsesteknologi til at matche disse billeder med billeder af personer, som politiet tidligere har samlet i en database (en såkaldt beskrivelsesdatabase, der består af mistænkte og tidligere dømte). Beskrivelsesdatabasen er til denne procedure – midlertidigt og i et isoleret miljø – analyseret med ansigtsgenkendelsesteknologi for at kunne gennemføre matchningsprocessen. For at minimere indgrebet i de matchede personers rettigheder og interesser har et meget begrænset antal ansatte i den kriminaltekniske afdeling tilladelse til at gennemføre den egentlige matchningsprocedure, adgangen til oplysningerne er begrænset til de ansatte, der har fået adgang til den specifikke fil, og der foretages en manuel kontrol af resultaterne, inden resultaterne sendes til den efterforskningsansvarlige medarbejder. De biometriske data videresendes ikke uden for det kontrollerede, isolerede miljø. Kun resultatet og billedet (ikke den biometriske skabelon) bruges videre i undersøgelsen. Medarbejderne modtager specifik uddannelse i reglerne og procedurerne for denne behandling, og al behandling af personoplysninger og biometriske data er tilstrækkeligt specificeret i den nationale lovgivning.

Kilde til oplysninger:

- Typer af registrerede: ☒ mistænkte, der er identificeret på grundlag af optagelser fra kameraovervågning
- Kilde til billede: ☒ offentligt tilgængelige rum ☒ internettet
- Forbindelse til kriminalitet: ☒ direkte tidsmæssig
  ☒ direkte geografisk

- Metode til indsamling af oplysninger: ☒ fjernovervågning
- Kontekst – påvirkes andre grundlæggende rettigheder: Ja, dvs.: ☒ forsamlingsfrihed ☒ ytringsfrihed ☒ andre: __

Referencedatabase (som de indsamlede oplysninger sammenlignes med):

- Specificitet: ☒ specifikke databaser relateret til kriminalitetsområdet.

Algoritme:

- Behandlingstype: ☒ 1:mange-identifikation

Resultat:

- Indvirkning: ☒ direkte (f.eks. hvis den registrerede bliver anholdt eller afhørt)
- Automatiseret afgørelse: ☒ NEJ

Retlig analyse:

- Gældende retlig ramme: ☒ specifik national lovgivning for denne behandling (ansigtsgenkendelse) for den pågældende kompetente myndighed

4.2. Gældende retlige rammer

I dette scenarie er det specificeret i den nationale lovgivning, at biometriske data kan bruges til at udføre kriminaltekniske analyser, når det er strengt nødvendigt for at opnå formålet med at identificere mistænkte, der begår en alvorlig forbrydelse, gennem matchning af billederne i beskrivelsesdatabasen. Den nationale lovgivning specificerer, hvilke data der kan behandles, samt procedurerne for sikring af personoplysningernes integritet og fortrolighed og procedurerne for deres tilintetgørelse, hvorved der gives tilstrækkelige garantier mod risikoen for misbrug og vilkårlighed.

4.3. Nødvendighed og proportionalitet

Anvendelse af ansigtsgenkendelse er klart mere tidseffektiv end manuel matchning på det kriminaltekniske niveau. Den manuelle udvælgelse af billeder på forhånd begrænser indgrebet i forhold til at køre alt videomaterialet mod en database og kan derved differentiere og kun målrette mod de personer, der er omfattet af målet, dvs. bekæmpelse af alvorlig kriminalitet. Det er dog stadig vigtigt at overveje, om matchningen kan udføres manuelt inden for en rimelig tid, afhængigt af den foreliggende sag. Begrænsningen af personer med adgang til teknologien og personoplysningerne mindsker indvirkningen på retten til privatlivets fred og databeskyttelse, ligesom det forhold at de biometriske skabeloner ikke lagres eller anvendes senere i forbindelse med undersøgelsen. Den manuelle kontrol af resultatet betyder også en reduceret risiko for falske positive resultater.

4.4. Konklusion

Det er vigtigt, at den nationale lovgivning giver et passende retsgrundlag for behandlingen af biometriske data samt for den nationale database, som matchningen finder sted med. I dette scenarie er der indført flere foranstaltninger for at begrænse indgrebet i databeskyttelsesrettighederne, såsom betingelserne for brug af ansigtsgenkendelsesteknologi, der er specificeret i retsgrundlaget, antallet af personer med adgang til teknologien og de biometriske data, manuelle kontroller osv. Ansigtsgenkendelsesteknologien forbedrer i væsentlig grad effektiviteten i efterforskningsarbejdet i politiets kriminaltekniske afdeling og er baseret på lovgivning, der giver politiet mulighed for at behandle biometriske data, når det er absolut nødvendigt, og kan derfor inden for disse rammer betragtes som et lovligt indgreb i individets rettigheder.

5 SCENARIE 5

5.1. Beskrivelse

Biometrisk fjernidentifikation er, når personers identitet fastslås ved hjælp af biometriske identifikatorer (ansigtsbillede, gangart, iris osv.) på afstand, i et offentligt rum og på en kontinuerlig eller løbende måde ved at kontrollere dem mod (biometriske) data, der er gemt i en database[89]. Biometrisk fjernidentifikation udføres i realtid, hvis optagelsen af billedmaterialet, sammenligningen og identifikationen sker uden væsentlig forsinkelse.

Forud for hver anvendelse af biometrisk identifikation i realtid udarbejder politiet en overvågningsliste over personer af interesse, der indgår i en efterforskning. Den indeholder ansigtsbilleder af enkeltindivider. Baseret på efterretninger, der tyder på, at disse individer vil være i et bestemt område, såsom et indkøbscenter eller en offentlig plads, beslutter politiet, hvornår, hvor og hvor længe den biometriske fjernidentifikation skal anvendes.

På aktionsdagen indsættes en politivogn som kontrolcenter med en ledende politimedarbejder om bord. Vognen indeholder skærme, der viser optagelser fra overvågningskameraer i nærheden, enten installeret på ad hoc-basis eller ved at forbinde til videostrømme fra allerede installerede kameraer. Når fodgængere går forbi kameraerne, isolerer teknologien ansigtsbilleder, konverterer dem til en biometrisk skabelon og sammenligner disse med de biometriske skabeloner for dem, der er på overvågningslisten.

Hvis der registreres et potentielt match mellem overvågningslisten og de personer, der passerer kameraerne, sendes en alarm til betjentene i bilen, som derefter informerer betjentene på stedet, hvis alarmen er positiv, f.eks. via en radioenhed. Betjenten på stedet vil så beslutte, om styrkerne skal gribe ind, nærme sig eller i sidste ende anholde personen. De foranstaltninger, der træffes af betjenten på stedet, registreres. I tilfælde af en diskret kontrol gemmes de indsamlede oplysninger (f.eks. hvem personen er sammen med, hvilket tøj de har på, og hvor de er på vej hen).

En national lovgivning, der henvises til, indeholder en generisk bestemmelse, hvorefter behandling af biometriske data med det formål entydigt at identificere en fysisk person er tilladt, hvis det er strengt nødvendigt og underlagt passende garantier for den pågældende persons rettigheder og frihedsrettigheder.

Kilde til oplysninger:

- Typer af registrerede: ☒ alle personer
- Kilde til billede: ☒ offentligt tilgængelige rum
- Tilknytning til kriminalitet: ☒ ikke nødvendigvis direkte geografisk eller tidsmæssig forbindelse
- Metode til indsamling af oplysninger: ☒ fjernovervågning
- Kontekst – påvirker andre grundlæggende rettigheder: Ja, dvs.: ☒ forsamlingsfrihed ☒ ytringsfrihed ☒ andet
- Tilgængelige yderligere kilder til information om den registrerede: ☒ andet: ikke udelukket (f.eks. brug af hæveautomater eller besøg i butikker)

Referencedatabase (som de indsamlede oplysninger sammenlignes med):

- Specificitet: ☒ specifikke databaser relateret til kriminalitetsområdet.

Algoritme:

[89] https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

- Behandlingstype: ☒ 1:mange-identifikation

Resultat:

- Indvirkning: ☒ direkte (f.eks. den registrerede bliver arresteret, afhørt)
- Automatiseret afgørelse: ☒ NEJ
- Opbevaringsvarighed: indtil alle mulige undersøgelser er afsluttet

Retlig analyse:

- Type af forudgående information til den registrerede: ☒ på retshåndhævende myndigheders hjemmeside generelt
- Gældende retlig ramme: ☒ Retshåndhævelsesdirektivet er primært kopieret til national lovgivning ☒ Generisk national lovgivning for retshåndhævende myndigheders brug af biometriske data

5.2. Gældende retlige rammer

Retsgrundlag, der blot gentager den generelle bestemmelse i artikel 10 i retshåndhævelsesdirektivet, er ikke tilstrækkeligt klare i deres ordlyd til at give enkeltpersoner en passende indikation af de betingelser og omstændigheder, hvorunder de retshåndhævende myndigheder har beføjelse til at anvende optagelser fra overvågningskameraer på offentlige steder til at oprette en biometrisk skabelon af deres ansigt og sammenligne den med politiets databaser. Den retlige ramme, der er etableret i dette scenarie, opfylder derfor ikke minimumskravene til at fungere som et juridisk grundlag[90].

5.3. Nødvendighed og proportionalitet

Kravene til nødvendighed og proportionalitet bliver højere, jo mere omfattende indgrebet er. Biometrisk fjernidentifikation på offentlige steder har flere konsekvenser for de grundlæggende rettigheder:

Scenarierne indebærer overvågning af alle forbipasserende i det pågældende offentlige rum. Det påvirker således i alvorlig grad befolkningernes rimelige forventning om at være anonyme i det offentlige rum[91]. Dette er en forudsætning for mange aspekter af den demokratiske proces, såsom beslutningen om at melde sig ind i en borgerforening, besøge forsamlinger og møde mennesker med alle sociale og kulturelle baggrunde, deltage i en politisk protest og besøge steder af enhver slags. Begrebet anonymitet i det offentlige rum er afgørende for at kunne indsamle og udveksle oplysninger og idéer frit. Det medvirker til at bevare mangfoldigheden af synspunkter, friheden til at deltage i fredelige forsamlinger, foreningsfriheden og beskyttelsen af mindretal og er til støtte for principperne om magtens tredeling og om kontrol og balancer. Underminering af begrebet anonymitet i det offentlige rum kan medføre mærkbare afskrækkende virkninger for borgerne. De kan muligvis afholde sig fra visse former for adfærd, som ligger inden for rammerne af et frit og åbent samfund. Det ville

[90] I tilfælde, hvor et videnskabeligt projekt, der har til formål at undersøge anvendelsen af ansigtsgenkendelsesteknologi, vil skulle behandle personoplysninger, men en sådan behandling ikke falder ind under artikel 4, stk. 3, i retshåndhævelsesdirektivet eller falder uden for EU-rettens anvendelsesområde, finder den generelle forordning om databeskyttelse anvendelse. I tilfælde af pilotprojekter, der vil blive efterfulgt af retshåndhævelsesoperationer, vil retshåndhævelsesdirektivet stadig finde anvendelse.

[91] Databeskyttelsesrådets svar til medlemmer af Europa-Parlamentet vedrørende appen om ansigtsgenkendelse udviklet af Clearview AI, 10. juni 2020, ref.: OUT2020-0052.

påvirke den almene interesse, da et demokratisk samfund forudsætter, at borgerne har selvbestemmelse og deltager i den demokratiske proces.

Hvis en sådan teknologi anvendes, vil blot det at gå på gaden, til metroen eller til bageren i det berørte område føre til indsamling af personlige, herunder biometriske data, af de retshåndhævende myndigheder og, i det første scenarie, også til matchning med politiets databaser. En situation, hvor det samme ville blive gjort ved at tage fingeraftryk, ville være klart ude af proportioner.

Antallet af berørte registrerede er ekstremt højt, da alle, der passerer det pågældende offentlige område, er berørt. Endvidere ville scenarierne indebære automatiseret massebehandling af biometriske data og også massematchning af biometriske data med politiets databaser.

I henhold til europæisk retspraksis er masseovervågning forbudt (f.eks. betragtede Menneskerettighedsdomstolen i S. og Marper mod Det Forenede Kongerige den vilkårlige lagring af biometriske data som et uforholdsmæssigt indgreb i retten til privatlivets fred, da det ikke betragtes som nødvendigt i et demokratisk samfund).

Biometrisk fjernidentifikation er så tæt knyttet til masseovervågning, at der ikke findes pålidelige begrænsningsmidler. Det er væsensforskelligt fra videoovervågning som sådan, da den mulige brug af videooptagelser uden biometrisk identifikation allerede udgør en stærk indgriben, men samtidig begrænset, hvorimod anvendelse af ansigtsgenkendelsesteknologi medfører, at den i forvejen udbredte brug af videoovervågningssystem som den vigtigste datakilde undergår en kvalitetsændring. Navnlig med hensyn til de forventelige afskrækkende virkninger vil eventuelle begrænsninger i anvendelsen af de allerede eksisterende videoovervågningsanlæg desuden ikke være synlige og vil således ikke vække tillid hos offentligheden.

Biometrisk fjernidentifikation fra politimyndigheders side behandler alle som potentielle mistænkte. I en retsstat formodes borgerne imidlertid at følge lovgivningen, indtil en forseelse kan bevises. Dette princip afspejles også delvist i retshåndhævelsesdirektivet, som understreger behovet for så vidt muligt at sondre mellem behandling af dømte eller mistænkte, i hvilket tilfælde de retshåndhævende myndigheder skal have "*væsentlig grund til at tro, at de har begået eller vil begå en strafbar handling*" (artikel 6, litra a), i retshåndhævelsesdirektivet), i forhold til dem, der ikke er dømt eller mistænkt for strafbare aktiviteter.

På transportknudepunkter eller offentlige rum vil retshåndhævende myndigheder ved hjælp af en teknologi, der er i stand til entydigt at identificere en enkelt person og spore og analysere dennes opholdssted og bevægelser, kunne afsløre endog de mest følsomme oplysninger om en person (selv seksuelle præferencer, religion, helbredsproblemer). Med dette følger en enorm risiko for ulovlig adgang til og brug af data.

Installation af systemer, der gør det muligt at afdække selve kernen i den enkeltes adfærd og karakteristika, fører til stærke afskrækkende virkninger. Det får folk til at overveje, om de skal deltage i en bestemt begivenhed, og det skader den demokratiske proces. At møde og blive set offentligt med en bestemt ven, der er kendt for at have problemer med politiet eller opføre sig på en unik måde, kan også ses som kritisk, da alt dette vil føre til tiltrækning af systemets algoritme og dermed af ordensmagten.

Det er umuligt at beskytte sårbare registrerede som børn. Desuden påvirkes personer, der har en professionel interesse i – og ofte en tilsvarende juridisk forpligtelse til – at holde deres kontakter fortrolige, såsom journalister, advokater og gejstlige. Dette kan f.eks. føre til afsløringer af kilder og journalister eller af det faktum, at en person konsulterer en kriminalforsvarsadvokat. Problemet

gælder ikke kun tilfældige offentlige steder, hvor f.eks. journalister og deres kilder mødes, men naturligvis også i de offentlige rum, der anvendes for at nærme sig og få adgang til institutioner eller fagfolk i denne henseende.

Desuden kan folks manglende tillid til ansigtsgenkendelsesteknologi få dem til at ændre deres adfærd og undgå steder, hvor ansigtsgenkendelsesteknologi indsættes, og dermed undgå at deltage i det sociale liv og i kulturelle arrangementer. Afhængigt af omfanget af indsættelsen af ansigtsgenkendelsesteknologi kan konsekvenserne for mennesker være så betydelige, at det påvirker deres evne til at leve et værdigt liv[92].

Der er derfor stor sandsynlighed for at påvirke kernen – den urørlige kerne – i retten til beskyttelse af personoplysninger. Stærke indikationer (jf. afsnit 3.1.3.2 i retningslinjerne) er navnlig følgende: I stor skala behandles menneskers entydige biologiske egenskaber automatisk af retshåndhævende myndigheder med algoritmer, der er baseret på plausibilitet, og hvor resultaterne kun i ringe omfang er åbne for forklaring. Begrænsningerne i retten til privatliv og databeskyttelse pålægges uanset personens individuelle adfærd eller de omstændigheder, der vedrører ham eller hende. Statistisk set er næsten alle de registrerede, der er berørt af dette indgreb, lovlydige personer. Der er kun begrænsede muligheder for at give information til de registrerede. I de fleste tilfælde vil det først være muligt efterfølgende at indbringe sagen for domstolene.

Tillid til et system baseret på plausibilitet og med begrænset forklarlighed kan føre til uklare ansvarsplaceringer og mangel på retsmidler og kan udgøre et incitament til uagtsomhed.

Når et sådant system, som også kan anvendes på eksisterende overvågningskameraer, anvendes med meget få anstrengelser og uden at være synlig for den enkelte, kan det misbruges og sættes i stand til systematisk og hurtigt at udarbejde lister over personer afhængigt af etnisk oprindelse, køn, religion osv. Princippet om behandling af personoplysninger i forhold til forud fastsatte kriterier såsom personens opholdssted og rejserute er tidligere behandlet[93] og kan give anledning til forskelsbehandling.

I overensstemmelse med følsomheden, den forenklede karakter og mængden af behandlede oplysninger er det sandsynligt, at systemer til fjerngenkendelse af ansigter på offentligt tilgængelige steder kan misbruges med skadelige virkninger for de berørte personer. Sådanne data kan også let indsamles og misbruges til at lægge pres på nøgleaktører i princippet om kontrol og balance, såsom den politiske opposition, embedspersoner og journalister.

Endelig har systemer med ansigtsgenkendelsesteknologi en tendens til at indeholde stærk forudindtagethed med hensyn til race og køn: falske positive resultater påvirker uforholdsmæssigt farvede og kvinder[94], hvilket resulterer i forskelsbehandling. Politiets foranstaltninger efter et falsk positivt resultat i form af ransagninger og anholdelser stigmatiserer disse grupper yderligere.

---

92 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, s. 20.

93 Jf. artikel 6 i Europa-Parlamentets og Rådets direktiv (EU) 2016/681 af 27. april 2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet samt artikel 33 i Europa-Parlamentets og Rådets forordning (EU) 2018/1240 af 12. september 2018 om oprettelse af et europæisk system vedrørende rejseinformation og rejsetilladelse (ETIAS) og om ændring af forordning (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 og (EU) 2017/2226.

94 https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf,
http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

5.4. Konklusion

De førnævnte scenarier vedrørende fjernbehandling af biometriske data i det offentlige rum til identifikationsformål skaber ikke en rimelig balance mellem de konkurrerende private og offentlige interesser og udgør dermed et uforholdsmæssigt indgreb i den registreredes rettigheder i henhold til artikel 7 og 8 i chartret.

6 SCENARIE 6

6.1. Beskrivelse

En privat enhed leverer en applikation, hvor ansigtsbilleder "skrabes" fra internettet for at oprette en database. Brugeren, f.eks. politiet, kan derefter uploade et billede, og ved hjælp af biometrisk identifikation vil applikationen forsøge at matche det med ansigtsbillederne eller de biometriske skabeloner i databasen.

En lokal politiafdeling efterforsker en forbrydelse, der er optaget på video, hvor en række potentielle vidner og mistænkte ikke kan identificeres ved at matche indsamlede oplysninger med interne databaser eller efterretninger. Personerne er efter de indsamlede oplysninger ikke registreret i nogen eksisterende politidatabase. Politiet beslutter at anvende et værktøj som beskrevet ovenfor, der stilles til rådighed af en privat virksomhed, til at identificere enkeltpersoner via biometrisk identifikation.

Kilde til oplysninger:

- Typer af registrerede: ☒ alle borgere (vidner) ☒ dømte ☒ mistænkte
- Kilde til billede: ☒ videooptagelser fra et offentligt sted eller indsamlet andetsteds i forbindelse med en forundersøgelse.
- Forbindelse til kriminalitet: ☒ ikke nødvendigt
- Metode til indsamling af oplysninger: ☒ fjernovervågning
- Kontekst – påvirker andre grundlæggende rettigheder: Ja, dvs.: ☒ forsamlingsfrihed ☒ ytringsfrihed ☒ andet: __

Referencedatabase (som de indsamlede oplysninger sammenlignes med):

- Specificitet: ☒ databaser til generelle formål udfyldt med data fra internettet

Algoritme:

- Behandlingstype: ☒ 1:mange-identifikationer

Resultat:

- Indvirkning ☒ direkte (f.eks. den registrerede bliver arresteret, afhørt, diskriminerende adfærd)
- Automatiseret afgørelse: ☒ NEJ

Retlig analyse:

- Type af forudgående information til den registrerede: ☒ Nej

6.2. Gældende retlige rammer

Når en privat enhed leverer en tjeneste, der omfatter behandling af personoplysninger, som den bestemmer formål med og midler til (i dette tilfælde scraping af billeder fra internettet for at oprette en database), skal denne private enhed have et retsgrundlag for behandlingen. Desuden skal de retshåndhævende myndigheder, der beslutter at bruge denne tjeneste til sit formål, have et

retsgrundlag for behandlingen, som de derefter fastsætter formål med og midler til. For at de retshåndhævende myndigheder kan behandle biometriske data, skal der være en retlig ramme, der præciserer formålet, de personoplysninger, der skal behandles, formålene med behandlingen og procedurerne for at sikre personoplysningernes integritet og fortrolighed samt procedurerne for tilintetgørelse heraf.

Dette scenarie indebærer masseindsamling af personlige data fra personer, der ikke er klar over, at deres data bliver indsamlet. En sådan behandling kan kun være lovlig under ganske særlige omstændigheder. Afhængigt af, hvor databasen er placeret, kan brugen af en sådan tjeneste medføre overførsel af personoplysninger og/eller særlige kategorier af personoplysninger uden for EU (af politiet, f.eks. ved at "sende" ansigtsbilleder, der stammer fra overvågningsvideoen eller er indsamlet på anden måde), hvilket forudsætter tilstedeværelse af særlige betingelser, jf. artikel 39 i retshåndhævelsesdirektivet.

Der er ingen specifikke regler i dette scenarie, der tillader denne behandling fra de retshåndhævende myndigheders side.

6.3. Nødvendighed og proportionalitet

De retshåndhævende myndigheders brug af tjenesten betyder, at personlige data deles med en privat enhed, der bruger en database, hvor personlige data indsamles ubegrænset og i stor skala. Der er ingen forbindelse mellem de indsamlede personoplysninger og de retshåndhævende myndigheders forfulgte mål. De retshåndhævende myndigheders deling af data med den private enhed betyder også, at myndighederne ikke har kontrol over de data, der behandles af den private enhed, og at det er meget vanskeligt for de registrerede at udøve deres rettigheder, da de ikke vil være klar over, at deres data behandles på denne måde. Dette medfører meget strenge kriterier for en situation, hvor det overhovedet kan komme på tale, at en sådan behandling kan finde sted. Det er tvivlsomt, om et mål ville opfylde kravene i direktivet, da eventuelle undtagelser fra og begrænsninger af retten til privatlivets fred og databeskyttelse kun finder anvendelse, når det er strengt nødvendigt. Den generelle interesse i effektivitet i bekæmpelsen af alvorlige forbrydelser kan ikke i sig selv retfærdiggøre behandling, hvor så store mængder data indsamles vilkårligt. Denne behandling ville derfor ikke opfylde kravene om nødvendighed og proportionalitet.

6.4. Konklusion

Manglen på klare, præcise og forudsigelige regler, der opfylder kravene i direktivets artikel 4 og 10, og manglen på bevis for, at denne behandling er strengt nødvendig for at nå de tilsigtede mål, fører til den konklusion, at brugen af denne applikation ikke ville opfylde kravene om nødvendighed og proportionalitet og ville betyde et uforholdsmæssigt indgreb i de registreredes ret til respekt for privatliv og beskyttelse af personoplysninger i henhold til chartret.