Riktlinjer

Translations proofread by EDPB Members. This language version has not yet been proofread.

Riktlinjer 05/2022 om användningen av teknik för ansiktsigenkänning på brottsbekämpningsområdet

Version 2.0

Antagna den 26 april 2023

Versionshistorik

Version 1.0	12 maj 2022	Antagande av riktlinjerna inför offentligt samråd
Version 2.0	26 april 2023	Antagande av riktlinjerna efter offentligt samråd

Innehåll

SAMMANFATTNING

Allt fler brottsbekämpande myndigheter tillämpar eller har för avsikt att tillämpa teknik för ansiktsigenkänning. Tekniken kan användas för att **autentisera** eller **identifiera** en person med hjälp av videofilmer (t.ex. från övervakningskameror) eller fotografier. Den kan användas för olika ändamål, bland annat för att söka efter personer i polisens bevakningslistor eller för att övervaka en persons förflyttningar i det offentliga rummet.

Ansiktsigenkänningstekniken bygger på behandling av **biometriska uppgifter** och inbegriper därför behandling av vissa kategorier av personuppgifter. I många fall används **artificiell intelligens** (AI) eller maskininlärning som komplement. Detta möjliggör en storskalig databehandling, men medför även en risk för diskriminering och felaktiga resultat. Tekniken kan användas vid individuella kontroller, men även i stora folksamlingar och i anslutning till viktiga transportknutpunkter.

Ansiktsigenkänningsteknik är ett **känsligt verktyg för brottsbekämpande myndigheter**. Brottsbekämpande myndigheter är verkställande myndigheter med suveräna befogenheter. Ansiktsigenkänningsteknik riskerar att inkräkta på de grundläggande rättigheterna – inte bara rätten till skydd av personuppgifter – och kan även påverka vår sociala och demokratiska politiska stabilitet.

För att säkerställa skyddet av personuppgifter i samband med brottsbekämpning måste **kraven i brottsdatadirektivet** vara uppfyllda. En viss ram för användningen av ansiktsigenkänningsteknik fastställs i brottsdatadirektivet, särskilt artikel 3.13 (begreppet *biometriska uppgifter*), artikel 4 (principer för behandling av personuppgifter), artikel 8 (laglig behandling av personuppgifter), artikel 10 (behandling av särskilda kategorier av personuppgifter) och artikel 11 (automatiserat individuellt beslutsfattande).

Det finns även andra grundläggande rättigheter som kan påverkas av tillämpningen av ansiktsigenkänningsteknik. Därför är **Europeiska unionens stadga om de grundläggande rättigheterna** (*stadgan*) avgörande för tolkningen av brottsdatadirektivet. Detta gäller särskilt rätten till skydd av personuppgifter i artikel 8 i stadgan, men även rätten till respekt för privatlivet, som fastställs i artikel 7 i stadgan.

Lagstiftningsåtgärder som utgör en rättslig grund för behandling av personuppgifter har en direkt inverkan på de rättigheter som garanteras i artiklarna 7 och 8 i stadgan. Behandlingen av biometriska uppgifter utgör under alla omständigheter ett allvarligt intrång i sig. Detta är inte beroende av utfallet, t.ex. en positiv matchning. Varje begränsning av utövandet av grundläggande rättigheter och friheter ska vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter.

Den rättsliga grunden måste vara **tillräckligt tydlig** för att ge medborgarna kännedom om de villkor och omständigheter under vilka myndigheterna har befogenhet att tillgripa åtgärder för insamling av uppgifter och hemlig övervakning. Om den allmänna klausulen i artikel 10 i brottsdatadirektivet införlivas direkt i nationell rätt riskerar den rättsliga grunden att bli otydlig och oförutsägbar.

Innan den nationella lagstiftaren skapar en ny rättslig grund för någon form av behandling av biometriska uppgifter med användning av ansiktsigenkänning bör den behöriga tillsynsmyndigheten för dataskydd **rådfrågas**.

Lagstiftningsåtgärderna måste vara **lämpliga** för att uppnå de legitima mål som eftersträvas med den berörda lagstiftningen. Ett **mål av allmänt samhällsintresse** – hur grundläggande det än är – kan inte i sig motivera en begränsning av en grundläggande rättighet. Lagstiftningsåtgärderna bör **göra åtskillnad** och vara inriktade på de personer som omfattas av dem mot bakgrund av målet, t.ex.

bekämpning av specifik grov brottslighet. Om åtgärden generellt omfattar samtliga personer utan sådana åtskillnader, begränsningar eller undantag förstärker den intrånget. Intrånget förstärks även om behandlingen av uppgifter omfattar en betydande del av befolkningen.

Uppgifterna måste behandlas på ett sätt som säkerställer att EU:s regler och principer för dataskydd är tillämpliga och effektiva. Vid **bedömningen av nödvändighet och proportionalitet** är det även nödvändigt att i varje enskild situation identifiera och överväga alla de möjliga konsekvenserna för andra grundläggande rättigheter. Om uppgifterna behandlas systematiskt utan de registrerades vetskap kommer de sannolikt att ge en **allmän känsla av ständig övervakning**. Detta kan ha en avskräckande effekt på några eller alla berörda grundläggande rättigheter, däribland människans värdighet enligt artikel 1 i stadgan, tankefrihet, samvetsfrihet och religionsfrihet enligt artikel 10 i stadgan, yttrandefrihet enligt artikel 11 i stadgan samt mötes- och föreningsfrihet enligt artikel 12 i stadgan.

Behandling av särskilda kategorier av uppgifter, däribland biometriska uppgifter, kan endast betraktas som **absolut nödvändig** (artikel 10 i brottsdatadirektivet) om intrånget i skyddet av personuppgifter och dess begränsningar begränsas till vad som är absolut nödvändigt, dvs. ofrånkomligt, och utesluter all behandling av allmän eller systematisk karaktär.

Det faktum att ett fotografi har **offentliggjorts på ett tydligt sätt** (artikel 10 i brottsdatadirektivet) av den registrerade innebär inte att de biometriska uppgifter som kan hämtas från fotografiet med särskilda tekniska hjälpmedel anses ha offentliggjorts på ett tydligt sätt. Standardinställningarna för en tjänst, t.ex. att mallar görs allmänt tillgängliga eller att det inte finns några valmöjligheter, dvs. att mallar offentliggörs utan att användaren kan ändra inställningarna, bör inte på något sätt tolkas som att uppgifterna har offentliggjorts på ett tydligt sätt.

Genom artikel 11 i brottsdatadirektivet fastställs en ram för **automatiserat individuellt beslutsfattande**. Användningen av ansiktsigenkänningsteknik berör särskilda kategorier av uppgifter som kan leda till profilering beroende på teknikens tillämpning och dess ändamål. Under alla omständigheter ska profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter vara förbjuden i enlighet med unionsrätten och artikel 11.3 i brottsdatadirektivet.

I artikel 6 i brottsdatadirektivet fastställs behovet av att **skilja mellan olika kategorier av registrerade**. När det gäller registrerade för vilka det inte finns något som tyder på att deras agerande kan ha en koppling, inte ens indirekt eller avlägsen, till det berättigade syftet enligt brottsdatadirektivet, kan ett intrång med största sannolikhet inte motiveras.

Enligt **principen om uppgiftsminimering** (artikel 4.1 e i brottsdatadirektivet) bör allt videomaterial som inte är relevant för behandlingens ändamål alltid raderas eller anonymiseras (t.ex. genom att sudda ut vissa delar så att de inte kan återskapas i efterhand) innan materialet används.

Den personuppgiftsansvarige måste noggrant överväga hur (eller om) kraven för **den registrerades rättigheter** kan uppfyllas innan en behandling med ansiktsigenkänningsteknik inleds, eftersom tekniken ofta innefattar behandling av särskilda kategorier av personuppgifter utan någon samverkan med den registrerade.

För att den registrerade ska kunna utöva sina rättigheter på ett effektivt sätt måste den personuppgiftsansvarige uppfylla sina **informationsskyldigheter** (artikel 13 i brottsdatadirektivet). Vid bedömningen av huruvida det rör sig om ett av de ”specifika fall” som avses i artikel 13.2 i brottsdatadirektivet måste flera faktorer beaktas, däribland om personuppgifterna samlas in utan den

registrerades vetskap, eftersom detta skulle vara det enda sättet för de registrerade att effektivt utöva sina rättigheter. Om beslutsfattandet endast bygger på ansiktsigenkänningsteknik måste de registrerade informeras om hur det automatiserade beslutsfattandet går till.

När det gäller **begäran om tillgång**, i fall där biometriska uppgifter även lagras och kopplas till en identitet med alfanumeriska uppgifter, bör den behöriga myndigheten, i linje med principen om uppgiftsminimering, ha möjlighet att godkänna en begäran om tillgång på grundval av en sökning med dessa alfanumeriska uppgifter utan någon ytterligare behandling av andras biometriska uppgifter (dvs. sökning med ansiktsigenkänningsteknik i en databas).

Riskerna för de registrerade är särskilt allvarliga om felaktiga uppgifter lagras i en polisdatabas och/eller delas med andra enheter. Den personuppgiftsansvarige ska **korrigera** lagrade uppgifter och system för ansiktsigenkänning i enlighet med detta (se även skäl 47 i brottsdatadirektivet).

Rätten till **begränsning** blir särskilt viktig när det gäller ansiktsigenkänningsteknik (som baseras på algoritmer och därmed aldrig visar ett slutgiltigt resultat) i situationer där stora mängder uppgifter samlas in och där identifieringens noggrannhet och kvalitet kan variera.

En **konsekvensbedömning avseende dataskydd** är ett obligatoriskt krav innan teknik för ansiktsigenkänning får användas (se artikel 27 i brottsdatadirektivet). I syfte att öka förtroendet och öppenheten rekommenderar Europeiska dataskyddsstyrelsen (EDPB) att resultaten av sådana bedömningar, eller åtminstone de viktigaste resultaten och slutsatserna, offentliggörs.

Användningen av ansiktsigenkänningsteknik medför i de flesta fall en hög risk för de registrerades rättigheter och friheter. Den myndighet som inför tekniken bör därför **samråda med** den behöriga tillsynsmyndigheten innan systemet tas i bruk.

Med tanke på de biometriska uppgifternas unika karaktär bör den myndighet som inför och/eller använder teknik för ansiktsigenkänning vara särskilt uppmärksam på **säkerheten i samband med behandlingen** i enlighet med artikel 29 i brottsdatadirektivet. Den brottsbekämpande myndigheten bör framför allt säkerställa att systemet uppfyller relevanta standarder och omfattar skyddsåtgärder för biometriska mallar. Principer och åtgärder för dataskydd måste ingå i tekniken innan behandlingen av personuppgifter påbörjas. Om en brottsbekämpande myndighet har för avsikt att tillämpa och använda ansiktsigenkänningsteknik från externa leverantörer måste den därför, t.ex. i samband med upphandlingen, säkerställa att endast teknik som bygger på principerna om **inbyggt dataskydd och dataskydd som standard** används.

Loggning (se artikel 25 i brottsdatadirektivet) är en viktig skyddsåtgärd för att kontrollera om behandlingen är tillåten, både internt (dvs. egenkontroll av den personuppgiftsansvarige/personuppgiftsbiträdet) och av externa tillsynsmyndigheter. När det gäller system för ansiktsigenkänning rekommenderas att loggar förs vid ändringar av referensdatabasen och vid identifierings- eller verifieringsförsök, däribland över användare, resultat och konfidensgrad. Loggning är emellertid bara en av de väsentliga delarna av den övergripande **principen om ansvarsskyldighet** (se artikel 4.4 i brottsdatadirektivet). Den personuppgiftsansvarige måste kunna visa att behandlingen är förenlig med de grundläggande dataskyddsprinciperna i artikel 4.1–4.3 i brottsdatadirektivet.

EDPB erinrar om sin och Europeiska datatillsynsmannens gemensamma **uppmaning om ett förbud** mot vissa typer av behandling i samband med 1) biometrisk fjärridentifiering av enskilda personer på offentligt tillgängliga platser, 2) AI-stödda system för ansiktsigenkänning som kategoriserar enskilda personer på grundval av deras biometriska kännetecken i kluster efter etniskt ursprung, kön, politiska

åsikter eller sexuell läggning eller andra diskrimineringsgrunder, 3) användning av ansiktsigenkänning eller liknande teknik för att dra slutsatser om en fysisk persons känslor och 4) behandling av personuppgifter i ett brottsbekämpande sammanhang som skulle bygga på en databas som uppdateras genom massinsamling av personuppgifter på ett urskillningslöst sätt, t.ex. genom ”skrapning” av fotografier och ansiktsbilder som är tillgängliga online.

En viktig skyddsåtgärd för de grundläggande rättigheterna är en **effektiv tillsyn** från de behöriga dataskyddsmyndigheternas sida. Medlemsstaterna måste därför se till att tillsynsmyndigheterna har lämpliga och tillräckliga resurser för att kunna fullgöra sitt uppdrag.

Dessa **riktlinjer riktar sig** till såväl beslutsfattare på EU-nivå och nationell nivå som brottsbekämpande myndigheter och deras tjänstemän som inför och använder system för ansiktsigenkänning. De riktar sig även till enskilda personer som är allmänt intresserade eller vill känna till sina rättigheter som registrerade.

Syftet med riktlinjerna är att informera om vissa egenskaper hos ansiktsigenkänningstekniken och den tillämpliga rättsliga ramen i samband med brottsbekämpning (i synnerhet brottsdatadirektivet).

- I riktlinjerna ingår ett **verktyg som kan användas vid en första klassificering av känsligheten hos ett visst användningsfall** (bilaga I).
- Riktlinjerna innehåller även **praktisk vägledning för brottsbekämpande myndigheter som vill upphandla och använda ett system för ansiktsigenkänning** (bilaga II).
- Avslutningsvis ges beskrivningar av typiska **användningsfall och en förteckning över relevanta överväganden**, särskilt när det gäller nödvändighets- och proportionalitetsprövningen (bilaga III).

1 INLEDNING

1. Ansiktsigenkänningsteknik kan användas för att automatiskt identifiera enskilda personer med hjälp av deras ansikte. Tekniken bygger ofta på artificiell intelligens, t.ex. maskininlärningsteknik. Sådan teknik provas och används allt oftare på olika områden av enskilda användare och privata organisationer samt inom offentlig förvaltning. Brottsbekämpande myndigheter förväntar sig också fördelar med användningen av ansiktsigenkänningsteknik. Den kan bidra med lösningar på relativt nya utmaningar, till exempel utredningar som omfattar en stor mängd inhämtade bevis, men även på kända problem som bristen på personal för observations- och sökuppgifter.

2. Det ökade intresset för ansiktsigenkänning beror till stor del på teknikens effektivitet och skalbarhet. Med detta följer de nackdelar som är förknippade med tekniken och dess tillämpning – även i stor skala. Möjligheten att analysera tusentals personuppgifter med en enda knapptryckning innebär också att det räcker med små effekter av algoritmisk diskriminering eller felidentifiering för att allvarligt påverka beteendet hos ett stort antal personer i deras dagliga liv. Själva omfattningen av behandlingen av personuppgifter, och i synnerhet biometriska uppgifter, är också en viktig del av ansiktsigenkänningstekniken, eftersom behandlingen är ett intrång i den grundläggande rätten till skydd av personuppgifter enligt artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*).

3. De brottsbekämpande myndigheternas tillämpning av ansiktsigenkänningsteknik kommer att få – och har till viss del redan fått – stora konsekvenser för enskilda individer och grupper av personer, däribland minoriteter. Dessa konsekvenser kommer även att ha stor inverkan på vårt sätt att leva tillsammans och på vår sociala och demokratiska politiska stabilitet, vilken till stor del bygger på

pluralism och politisk opposition. Rätten till skydd av personuppgifter är ofta en förutsättning för att garantera andra grundläggande rättigheter. Tillämpningen av ansiktsigenkänningsteknik riskerar att inkräkta på andra grundläggande rättigheter vid sidan av rätten till skydd av personuppgifter.

4. EDPB anser därför att det är viktigt att bidra till den pågående integreringen av ansiktsigenkänningsteknik på det brottsbekämpningsområde som omfattas av brottsdatadirektivet[1] och den nationella lagstiftning som införlivar det, och tillhandahåller dessa riktlinjer för detta ändamål. Riktlinjerna är avsedda att ge relevant information till såväl lagstiftare på EU-nivå och nationell nivå som brottsbekämpande myndigheter och deras tjänstemän när de inför och använder system för ansiktsigenkänning. Riktlinjernas tillämpningsområde är begränsat till ansiktsigenkänningsteknik. Andra former av personuppgiftsbehandling baserad på biometri som utförs av brottsbekämpande myndigheter kan emellertid medföra liknande eller andra risker för enskilda personer, grupper och samhället i stort, särskilt om uppgifterna behandlas på distans. Beroende på omständigheterna kan vissa aspekter av dessa riktlinjer utgöra en användbar källa även i dessa fall. Slutligen kan enskilda personer som är intresserade i allmänhet eller i egenskap av registrerade hitta viktig information, särskilt när det gäller sina rättigheter som registrerade.

5. Riktlinjerna består av ett huvuddokument och tre bilagor. I huvuddokumentet presenteras tekniken och den tillämpliga rättsliga ramen. Bilaga I innehåller en mall som underlättar identifieringen av de viktigaste aspekterna vid bedömningen av hur allvarligt intrånget i de grundläggande rättigheterna är för ett visst tillämpningsområde. I bilaga II ges praktisk vägledning för brottsbekämpande myndigheter som vill upphandla och använda ett system för ansiktsigenkänning. Beroende på ansiktsigenkänningsteknikens tillämpningsområde kan olika överväganden vara relevanta. Slutligen återfinns ett antal hypotetiska scenarier och relevanta överväganden i bilaga III.

2 TEKNIK

2.1 En biometrisk teknik, två skilda funktioner

6. Ansiktsigenkänning är en probabilistisk teknik som automatiskt känner igen personer utifrån deras ansikten för att autentisera eller identifiera dem.

7. Tekniken ingår i en bredare kategori av biometrisk teknik. Med biometri avses alla automatiserade processer som används för att identifiera en person genom att kvantifiera fysiska, fysiologiska eller beteendemässiga kännetecken (fingeravtryck, regnbågshinnans struktur, röst, gångstil, blodkärlsmönster osv.). Dessa kännetecken kallas *biometriska uppgifter*, eftersom de möjliggör eller bekräftar en unik identifiering av personen.

8. Detta är fallet med människors ansikten, eller mer specifikt den tekniska behandlingen av ansikten med hjälp av ansiktsigenkänningsutrustning. En bild av ett ansikte (ett fotografi eller en video), även kallat ett *biometriskt prov*, kan användas för att ta fram en digital återgivning av ansiktets unika kännetecken (en så kallad *mall*).

[1] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

9. En *biometrisk mall* är en digital återgivning av de unika kännetecken som har hämtats från ett biometriskt prov och kan lagras i en biometrisk databas[2]. Denna mall förväntas vara unik och specifik för varje person, och är i princip permanent över tid[3]. I igenkänningsfasen jämförs denna mall med andra mallar som tidigare har skapats eller beräknats direkt från biometriska prover, t.ex. ansikten som finns på en bild, på ett fotografi eller i ett videoklipp. *Ansiktsigenkänning* är därför ett förfarande i två steg: insamlingen av ansiktsbilden och dess omvandling till en mall, följt av igenkänningsfasen där ansiktsmallen jämförs med en eller flera andra mallar.

10. Liksom andra biometriska processer kan ansiktsigenkänning ha två olika funktioner:

- **Autentisering** av en person för att kontrollera att personen är den som han eller hon utger sig för att vara. I detta fall jämför systemet en tidigare lagrad biometrisk mall eller ett biometriskt prov (t.ex. på ett smartkort eller ett biometriskt pass) med ett enskilt ansikte, t.ex. ansiktet hos en person som kommer till en kontrollstation, för att kontrollera om det rör sig om samma person. Denna funktion bygger således på en jämförelse mellan två olika mallar. Detta kallas även ”en mot en-**verifiering**” (*1-to-1 verification*).

- **Identifiering** av en person i syfte att hitta personen i en grupp av individer, inom ett specifikt område, på en bild eller i en databas. I detta fall måste systemet behandla varje ansikte för att generera en biometrisk mall och sedan kontrollera om den stämmer överens med en känd person i systemet. Denna funktion bygger således på att en mall jämförs med en databas över mallar eller prover (referensmallar). Detta kallas även ”en mot många-identifiering” (*1-to-many identification*). Tekniken kan till exempel koppla en personuppgift (efternamn, förnamn) till ett ansikte om jämförelsen görs mot en databas bestående av fotografier med tillhörande efternamn och förnamn. Den kan även användas för att följa en person genom en folkmassa, utan att nödvändigtvis göra en koppling till personens fysiska identitet.

11. I båda fallen baseras tekniken för ansiktsigenkänning på en uppskattad matchning mellan olika mallar: den mall som jämförs och en eller flera referensmallar. I detta hänseende är tekniken probabilistisk, dvs. jämförelsen leder till en högre eller lägre sannolikhet för att personen verkligen är den person som ska autentiseras eller identifieras. Om sannolikheten överstiger ett visst tröskelvärde i systemet, som fastställts av användaren eller systemutvecklaren, kommer systemet att visa en matchning.

12. De två funktionerna – autentisering och identifiering – utförs separat, men båda bygger på en behandling av biometriska uppgifter som avser en identifierad eller identifierbar fysisk person och utgör därför en behandling av personuppgifter, mer specifikt behandling av särskilda kategorier av personuppgifter.

13. Ansiktsigenkänning ingår i en bredare uppsättning av tekniker för bearbetning av videobilder. Vissa videokameror kan filma personer inom ett avgränsat område, särskilt deras ansikten, men de kan inte användas för att identifiera olika individer automatiskt. Detsamma gäller för enkel fotografering; en kamera är inte ett ansiktsigenkänningssystem, eftersom fotografier av människor måste behandlas på ett särskilt sätt för att biometriska uppgifter ska kunna tas fram.

14. Enbart det faktum att så kallade smarta kameror kan känna igen ansikten innebär inte att de utgör ett system för ansiktsigenkänning. Digital teknik för att upptäcka onormala beteenden eller våldsamma händelser, eller för att känna igen ansiktsuttryck eller till och med silhuetter, väcker viktiga frågor kring

[2] *Guidelines on facial recognition* (inte översatt till svenska), rådgivande kommittén för konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter (konvention 108), Europarådet, juni 2021.
[3] Detta kan bero på typen av biometri och den registrerades ålder.

etik och effektivitet, men kan inte betraktas som biometriska system som behandlar särskilda kategorier av personuppgifter, såvida de inte syftar till att identifiera en unik person och den berörda behandlingen inte inbegriper andra särskilda kategorier av personuppgifter. Dessa exempel har viss koppling till ansiktsigenkänning och omfattas fortfarande av bestämmelserna om skydd av personuppgifter[4]. Dessutom kan denna typ av detekteringssystem användas tillsammans med andra system som syftar till att identifiera en person och därmed betraktas som en ansiktsigenkänningsteknik.

15. Till skillnad från exempelvis videoupptagnings- och videobehandlingssystem, som kräver installation av fysiska anordningar, är ansiktsigenkänning en programvarufunktion som kan implementeras i befintliga system (kameror, bilddatabaser m.m.). Denna funktion kan därför anslutas till eller kopplas samman med en mängd olika system och kombineras med andra funktioner. En sådan integrering i befintlig infrastruktur kräver särskild uppmärksamhet, eftersom den medför inneboende risker på grund av att ansiktsigenkänningstekniken kan vara störningsfri och lätt att dölja[5].

2.2 En mängd olika ändamål och tillämpningar

16. Utöver tillämpningsområdet för dessa riktlinjer och brottsdatadirektivet kan ansiktsigenkänning användas för en rad olika ändamål, både i kommersiella sammanhang och i frågor som rör allmän säkerhet eller brottsbekämpning. Tekniken kan användas i många olika sammanhang: i den personliga relationen mellan en användare och en tjänst (åtkomst till ett program), för åtkomst till en viss plats (fysisk filtrering) eller utan någon särskild begränsning i det offentliga rummet (ansiktsigenkänning i realtid). Den kan tillämpas på alla typer av registrerade: en kund som köper en tjänst, en anställd, en oskyldig åskådare, en efterlyst person eller någon som är föremål för rättsliga eller administrativa förfaranden m.fl. Vissa användningsområden är redan vanliga och utbredda, medan andra i nuläget befinner sig i experiment- eller utvecklingsstadiet. Dessa riktlinjer omfattar inte alla sådana användningsområden och tillämpningar, och EDPB påminner om att de endast får genomföras om de är förenliga med den tillämpliga rättsliga ramen, i synnerhet den allmänna dataskyddsförordningen och relevant nationell lagstiftning[6]. Även inom ramen för brottsdatadirektivet kan uppgifter som behandlas med hjälp av ansiktsigenkänningsteknik behandlas vidare för andra ändamål än autentisering eller identifiering, till exempel kategorisering.

17. Mer specifikt kan en skala av möjliga användningsområden övervägas beroende på vilken kontroll människor har över sina personuppgifter, vilka effektiva medel de har för att utöva denna kontroll och deras rätt till initiativ för att utlösa och använda denna teknik, vilka konsekvenserna kan bli (vid en eventuell igenkänning) samt omfattningen av den behandling som utförs. Ansiktsigenkänning med hjälp av en mall som lagras i en personlig enhet (t.ex. ett smartkort eller en smarttelefon), som används för autentisering av enhetens ägare och för strikt personligt bruk via ett särskilt gränssnitt, medför inte samma risker som exempelvis användning för identifieringsändamål i en okontrollerad miljö utan aktiv medverkan av de registrerade, där mallen för varje ansikte i övervakningsområdet jämförs med mallar från ett brett tvärsnitt av befolkningen som lagras i en databas. Mellan dessa två ytterligheter finns ett mycket brett spektrum av användningsområden och tillhörande frågor som rör skyddet av personuppgifter.

[4] Artikel 10 i brottsdatadirektivet (eller artikel 9 i den allmänna dataskyddsförordningen) är emellertid tillämplig på system som används för att kategorisera enskilda personer på grundval av deras biometriska kännetecken i kluster efter etniskt ursprung, politiska åsikter eller sexuell läggning eller andra särskilda kategorier av personuppgifter.

[5] Till exempel i kroppsburna kameror som allt oftare används i praktiken.

[6] Se även EDPB:s riktlinjer 3/2019 för behandling av personuppgifter genom videoenheter, som antogs den 29 januari 2020, för ytterligare vägledning.

18. För att ytterligare illustrera det sammanhang inom vilket ansiktsigenkänningsteknik för närvarande diskuteras eller genomförs, antingen för autentisering eller identifiering, anser EDPB att det är relevant att ge ett antal exempel. De nedanstående exemplen är endast beskrivande och bör inte betraktas som en preliminär bedömning av deras överensstämmelse med EU:s regelverk på dataskyddsområdet.

Exempel på autentisering genom ansiktsigenkänning

19. Autentisering kan utformas så att användarna har full kontroll över den, till exempel för att ge tillgång till tjänster eller tillämpningar i hemmet. Många använder tekniken för att låsa upp sin smarttelefon i stället för att ange ett lösenord.

20. Autentisering genom ansiktsigenkänning kan även användas för att kontrollera identiteten hos någon som vill ta del av offentliga eller privata tjänster från tredje part. Dessa processer gör det möjligt att skapa en digital identitet med hjälp av en mobilapp (på t.ex. en smarttelefon eller surfplatta) som sedan kan användas för att få tillgång till administrativa tjänster online.

21. Autentisering genom ansiktsigenkänning kan även användas för att kontrollera det fysiska tillträdet till en eller flera förutbestämda platser, till exempel ingångar till byggnader eller särskilda gränsövergångsställen. Denna funktion tillämpas exempelvis vid viss personuppgiftsbehandling i samband med gränspassage, där personer vid gränskontrollen jämförs med det ansikte som lagrats i deras identitetshandlingar (pass eller uppehållstillstånd).

Exempel på identifiering med hjälp av ansiktsigenkänning

22. Identifiering kan tillämpas på många olika sätt. Dessa omfattar särskilt, men är inte begränsade till, de användningsområden som anges nedan och som för närvarande bevakas, provas eller planeras i EU.

- Sökning i en databas med fotografier efter en oidentifierad person (t.ex. ett brottsoffer eller en misstänkt person).
- Övervakning av en persons förflyttningar i det offentliga rummet. Personens ansikte jämförs med de biometriska mallarna av personer som reser eller har rest i det övervakade området, till exempel när en väska lämnas obevakad eller efter att ett brott har begåtts.
- Rekonstruktion av en persons resa och efterföljande interaktioner med andra personer, genom en fördröjd jämförelse av samma händelser för att till exempel försöka identifiera deras kontakter.
- Biometrisk fjärridentifiering av efterlysta personer på offentliga platser. Alla ansikten som fångas av videokameror dubbelkollas i realtid mot säkerhetsstyrkornas databas.
- Automatisk igenkänning av personer på en bild, till exempel för att identifiera deras relationer i ett socialt nätverk. Bilden jämförs med mallarna för alla i nätverket som har samtyckt till denna funktion för att underlätta den personliga identifieringen av dessa relationer.
- Tillgång till tjänster, där vissa uttagsautomater känner igen sina kunder genom att jämföra ett ansikte som fångats av en kamera med bankens databas över ansiktsbilder.
- Spårning av en passagerares resa i ett visst skede av resan. Mallen beräknas i realtid för alla personer som har checkat in i vissa skeden av resan (t.ex. vid avlämningsplatser för bagage eller vid gaten) och jämförs med mallarna för personer som tidigare varit registrerade i systemet.

23. Bortsett från användningen av ansiktsigenkänningsteknik på brottsbekämpningsområdet kräver detta breda spektrum av tillämpningar en omfattande diskussion och en politisk strategi för att säkerställa konsekvens och överensstämmelse med EU:s regelverk på dataskyddsområdet.

2.3 Tillförlitlighet, noggrannhet och risker för de registrerade

24. Som all annan teknik kan ansiktsigenkänning innebära utmaningar i samband med dess genomförande. Detta gäller särskilt tillförlitligheten och effektiviteten vid autentisering eller identifiering, liksom den övergripande frågan om ”källdatans” kvalitet och noggrannhet samt resultatet av behandlingen med ansiktsigenkänningsteknik.

25. De särskilda risker för registrerade som dessa tekniska utmaningar medför är särskilt betydande eller allvarliga på brottsbekämpningsområdet med tanke på de möjliga (rättsliga eller andra) konsekvenserna för de registrerade som berörs av behandlingen. I detta sammanhang bör det understrykas att användningen av teknik för ansiktsigenkänning i efterhand inte är säkrare i sig, eftersom enskilda personer kan spåras över tid och rum. Användning i efterhand medför således också särskilda risker som måste bedömas från fall till fall[7].

26. Som Europeiska unionens byrå för grundläggande rättigheter påpekade i sin rapport från 2019 är det svårt att fastställa den nödvändiga noggrannhetsnivån i programvara för ansiktsigenkänning. Det finns många olika sätt att utvärdera och bedöma noggrannheten, till exempel beroende på uppgiften, ändamålet och sammanhanget. Om tekniken används på platser som besöks av miljontals människor – t.ex. tågstationer eller flygplatser – innebär en relativt liten andel fel (t.ex. 0,01 %)[8] att hundratals människor registreras felaktigt. Det är dessutom troligt att vissa kategorier av människor registreras felaktigt oftare än andra, såsom beskrivs i avsnitt 3. Det finns olika sätt att beräkna och tolka felfrekvenser, och det är viktigt att vara varsam. När det gäller noggrannhet och fel är frågor kring hur enkelt det är att lura systemet, t.ex. med falska ansiktsbilder (så kallad spoofing), särskilt viktiga för brottsbekämpningen[9].

27. I detta sammanhang erinrar EDPB om att ansiktsigenkänningsteknik, oavsett om den används för autentisering eller identifiering, inte ger ett slutgiltigt resultat, utan bygger på sannolikheten för att två ansikten, eller bilder av ansikten, motsvarar samma person[10]. Detta resultat försämras ytterligare om de biometriska prover som används för ansiktsigenkänningen är av låg kvalitet. Suddiga bilder, låg kameraupplösning, rörelser och svag belysning kan vara faktorer som påverkar kvaliteten. Andra aspekter med betydande inverkan på resultaten är prevalens och spoofing, t.ex. när brottslingar antingen försöker undvika kamerorna eller lura ansiktsigenkänningstekniken. Flera studier har visat att sådana statistiska resultat från algoritmisk bearbetning också kan vara föremål för systematiska fel, särskilt på grund av källdatans kvalitet och utbildningsdatabasernas utformning eller andra faktorer såsom platsen. Det är dessutom viktigt att belysa hur ansiktsigenkänningstekniken påverkar andra grundläggande rättigheter, däribland respekten för privatlivet och familjelivet, yttrande- och informationsfriheten samt mötes- och föreningsfriheten.

28. Det är därför viktigt att ansiktsigenkänningsteknikens tillförlitlighet och noggrannhet beaktas som kriterier vid bedömningen av efterlevnaden av centrala dataskyddsprinciper, i enlighet med artikel 4 i brottsdatadirektivet, särskilt när det gäller rättvisa och noggrannhet.

29. Samtidigt som EDPB understryker att uppgifter av hög kvalitet är avgörande för algoritmernas kvalitet betonar myndigheten att personuppgiftsansvariga, som en del av sin ansvarsskyldighet, måste göra regelbundna och systematiska utvärderingar av den algoritmiska behandlingen, i synnerhet för att

[7] Se exemplen i bilaga III.

[8] Denna noggrannhetsnivå kommer från den nämnda rapporten och återspeglar en nivå som är mycket högre än de nuvarande algoritmernas prestanda vid tillämpning av ansiktsigenkänningsteknik.

[9] *Facial recognition technology: fundamental rights considerations in the context of law enforcement* (inte översatt till svenska), Europeiska unionens byrå för grundläggande rättigheter, 21 november 2019.

[10] Denna sannolikhet kallas konfidensgrad.

säkerställa att resultatet av personuppgiftsbehandlingen är korrekt, rättvist och tillförlitligt. Personuppgifter som används för att utvärdera, träna och vidareutveckla system för ansiktsigenkänning får endast behandlas på grundval av en tillräcklig rättslig grund och i enlighet med de gemensamma dataskyddsprinciperna.

3 TILLÄMPLIG RÄTTSLIG RAM

30. Användningen av ansiktsigenkänningsteknik medför behandling av personuppgifter, däribland särskilda kategorier av uppgifter. Tekniken har även en direkt eller indirekt inverkan på ett antal grundläggande rättigheter som fastställs i EU-stadgan om de grundläggande rättigheterna. Detta är särskilt relevant på områdena brottsbekämpning och straffrätt. All ansiktsigenkänningsteknik bör därför användas i strikt överensstämmelse med den tillämpliga rättsliga ramen.

31. Följande information är avsedd att användas som stöd vid bedömningen av framtida lagstiftningsåtgärder och administrativa åtgärder samt från fall till fall vid genomförandet av befintlig lagstiftning som inbegriper teknik för ansiktsigenkänning. De respektive kravens relevans varierar beroende på de särskilda omständigheterna. Eftersom inte alla framtida omständigheter kan förutses ska detta endast betraktas som ett stöd och inte tolkas som en uttömmande uppräkning.

3.1 Den allmänna rättsliga ramen – Europeiska unionens stadga om de grundläggande rättigheterna och den europeiska konventionen om de mänskliga rättigheterna

3.1.1 Stadgans tillämplighet

32. Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*) riktar sig till unionens institutioner, organ och byråer samt till medlemsstaterna när de tillämpar unionsrätten.

33. En reglering av behandlingen av biometriska uppgifter för brottsbekämpande ändamål i enlighet med artikel 1.1 i brottsdatadirektivet väcker oundvikligen frågan om förenligheten med de grundläggande rättigheterna, särskilt respekten för privatliv och kommunikationer enligt artikel 7 i stadgan och rätten till skydd av personuppgifter enligt artikel 8 i stadgan.

34. Insamling och analys av videoinspelningar av fysiska personer, inbegripet deras ansikten, innebär att personuppgifter behandlas. Vid den tekniska behandlingen av bilden omfattar behandlingen även biometriska uppgifter. Den tekniska behandlingen av uppgifter om fysiska personers ansikten i förhållande till tid och rum gör det möjligt att dra slutsatser om de berörda personernas privatliv. Dessa slutsatser kan avse ras eller etniskt ursprung, hälsa, religion, dagliga vanor, permanent eller tillfällig bosättningsort, dagliga eller tillfälliga förflyttningar, vilka aktiviteter som utövas, personernas sociala relationer och vilka sociala miljöer de vistas i. Den stora mängd information som kan tas fram med hjälp av ansiktsigenkänningsteknik visar tydligt hur tekniken påverkar rätten till skydd av personuppgifter enligt artikel 8 i stadgan, men även rätten till privatliv enligt artikel 7 i stadgan.

35. Under dessa omständigheter är det inte heller otänkbart att insamlingen, analysen och vidarebehandlingen av de biometriska (ansikts-)uppgifterna i fråga kan begränsa människors handlingsfrihet, även om handlingen ligger helt inom ramen för ett fritt och öppet samhälle. Det kan även få allvarliga konsekvenser för människors utövande av sina grundläggande rättigheter, däribland rätten till tankefrihet, samvetsfrihet och religionsfrihet samt rätten till frihet att delta i fredliga sammankomster och till föreningsfrihet enligt artiklarna 1, 10, 11 och 12 i stadgan. Denna behandling

inbegriper även andra risker, däribland risken för missbruk av de personuppgifter som samlats in av de berörda myndigheterna till följd av olaglig åtkomst till och användning av personuppgifterna, säkerhetsöverträdelser osv. Riskerna beror ofta på behandlingen och dess omständigheter, till exempel risken för att polistjänstemän eller obehöriga parter kommer åt och använder uppgifterna på ett olagligt sätt. Vissa risker beror emellertid helt enkelt på de biometriska uppgifternas unika karaktär. Till skillnad från en adress eller ett telefonnummer är det omöjligt för en registrerad att ändra sina unika egenskaper, som ansiktet eller regnbågshinnan. Om obehöriga kommer åt de biometriska uppgifterna eller om det finns risk för att de offentliggörs oavsiktligt kan de inte längre användas som lösenord eller krypteringsnycklar. Uppgifterna skulle även kunna användas för annan obehörig övervakning av den registrerade.

3.1.2 Intrång i de rättigheter som fastställs i stadgan

36. Behandlingen av biometriska uppgifter utgör under alla omständigheter ett allvarligt intrång i sig. Detta är inte beroende av utfallet, t.ex. en positiv matchning. Behandlingen utgör ett intrång även om den biometriska mallen raderas omedelbart om jämförelsen mot en polisdatabas inte leder till någon träff.

37. Intrånget i de registrerades grundläggande rättigheter kan härröra från en rättsakt som antingen syftar till eller medför att de respektive grundläggande rättigheterna begränsas[11]. Det kan även vara resultatet av en handling av en offentlig myndighet med samma syfte eller verkan, eller av en privat aktör som enligt lag har anförtrotts att utöva offentlig makt och offentliga befogenheter.

38. En lagstiftningsåtgärd som utgör rättslig grund för behandling av personuppgifter är ett direkt ingrepp på de rättigheter som är garanterade genom artiklarna 7 och 8 i stadgan[12].

39. Användningen av biometriska uppgifter, och särskilt ansiktsigenkänningsteknik, påverkar i många fall även rätten till människans värdighet, som garanteras i artikel 1 i stadgan. Denna rätt innebär att enskilda personer inte får behandlas som rena objekt. Ansiktsigenkänningsteknik används för att beräkna existentiella och mycket personliga egenskaper, dvs. ansiktsdragen, och omvandla dem till en maskinläsbar form som kan användas som en mänsklig registreringsskylt eller ett id-kort. Tekniken gör därmed ansiktet till ett objekt.

40. Behandlingen kan även inkräkta på andra grundläggande rättigheter, däribland rättigheterna enligt artiklarna 10, 11 och 12 i stadgan, i den mån avskräckande effekter är antingen en avsikt med eller en effekt av de brottsbekämpande myndigheternas videoövervakning.

41. Det är dessutom viktigt att noga överväga de risker som användningen av ansiktsigenkänningsteknik inom brottsbekämpningen kan medföra när det gäller rätten till en opartisk domstol och presumtion för oskuld enligt artiklarna 47 och 48 i stadgan. Resultatet av tillämpningen av ansiktsigenkänningsteknik, t.ex. en matchning, leder inte alltid bara till att en person blir föremål för ytterligare polisövervakning, utan kan även vara avgörande bevis i en domstol. Brister i ansiktsigenkänningstekniken, till exempel snedvridning, diskriminering eller felaktig identifiering (så kallade falska positiva resultat) kan således få allvarliga konsekvenser även för straffrättsliga förfaranden. Dessutom kan resultatet av tillämpningen av ansiktsigenkänningsteknik ges särskild tyngd vid bevisvärderingen, även om det finns motstridiga bevis (så kallad automationssnedvridning).

[11] Europeiska unionens domstol, C-219/91 – Ter Voort, RoC 1992 I-05485, punkt 36f och Europeiska unionens domstol, C-200/96 – Metronome, RoC 1998 I-1953, punkt 28.
[12] Europeiska unionens domstol, C-594/12, punkt 36 och Europeiska unionens domstol, C-291/12, punkt 23 och följande.

3.1.3 Motivering av intrånget

42. Enligt artikel 52.1 i stadgan ska varje begränsning i utövandet av de grundläggande rättigheterna och friheterna vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av Europeiska unionen eller behovet av skydd för andra människors rättigheter och friheter.

3.1.3.1 Föreskrifter i lagstiftningen

43. I artikel 52.1 i stadgan fastställs kravet på en specifik rättslig grund. Denna rättsliga grund måste vara tillräckligt tydlig för att ge medborgarna kännedom om de villkor och omständigheter under vilka myndigheterna har befogenhet att tillgripa åtgärder för insamling av uppgifter och hemlig övervakning[13]. Den måste med rimlig tydlighet ange hur de offentliga myndigheterna ska utöva den relevanta bestämmanderätten så att enskilda personer garanteras den lägsta grad av skydd som de har rätt till enligt rättsstatsprincipen i ett demokratiskt samhälle[14]. Enligt lag måste det dessutom finnas tillräckliga garantier för att säkerställa att i synnerhet enskildas rättigheter enligt artikel 8 i stadgan respekteras. Dessa principer gäller även vid behandling av personuppgifter i samband med utvärdering, anpassning och vidareutveckling av system för ansiktsigenkänning.

44. Med tanke på att biometriska uppgifter som behandlas för att unikt identifiera en fysisk person utgör särskilda kategorier av uppgifter enligt artikel 10 i brottsdatadirektivet skulle de olika tillämpningarna av ansiktsigenkänningsteknik i de flesta fall kräva en särskild lag som exakt beskriver tillämpningen och villkoren för dess användning. Detta omfattar särskilt de olika typerna av brott och, i tillämpliga fall, en lämplig gräns för hur allvarliga dessa brott är, för att bland annat kunna utesluta mindre förseelser[15].

3.1.3.2 Det väsentliga innehållet i den grundläggande rätten till privatliv och skydd av personuppgifter som fastställs i artiklarna 7 och 8 i stadgan

45. Vid begränsningar av de grundläggande rättigheter som gäller i varje enskild situation måste det väsentliga innehållet i den särskilda rättigheten fortfarande respekteras. Det väsentliga innehållet avser kärnan i den relevanta grundläggande rättigheten[16]. Människans värdighet får inte kränkas ens i fall av begränsning av en rättighet[17].

46. Följande omständigheter är tecken på en möjlig överträdelse av den okränkbara kärnan:

- En bestämmelse som medför begränsningar oberoende av en persons individuella beteende eller undantagsfall[18].
- Det finns inte någon möjlighet att väcka talan vid domstol[19].
- Ingen hänsyn tas till den berörda individens omständigheter innan en allvarlig begränsning införs[20].

[13] Europeiska domstolen för de mänskliga rättigheterna, Shimovolos mot Ryssland, punkt 68 och Vukota-Bojić mot Schweiz.
[14] Europeiska domstolen för de mänskliga rättigheterna, Piechowicz mot Polen, punkt 212.
[15] Se t.ex. EU-domstolens domar i målen C-817/19 Ligue des droits humains, punkt 151 f och C-207/16 Ministerio Fiscal, punkt 56.
[16] Europeiska unionens domstol, C-279/09, RoC 2010 I-13849, punkt 60.
[17] Förklaringar avseende stadgan om de grundläggande rättigheterna, Avdelning I, Förklaring till artikel 1, EUT C 303, 14.12.2007, s. 17.
[18] Europeiska unionens domstol, C-601/15, punkt 52.
[19] Europeiska unionens domstol, C-400/10, RoC 2010 I-08965, punkt 55.
[20] Europeiska unionens domstol, C-408/03, RoC 2006 I-02647, punkt 68.

- När det gäller rättigheterna enligt artiklarna 7 och 8 i stadgan: Utöver en bred insamling av metadata för kommunikation kan förvärvandet av kunskap om innehållet i den elektroniska kommunikationen strida mot det väsentliga innehållet i dessa rättigheter[21].
- När det gäller rättigheterna enligt artiklarna 7, 8 och 11 i stadgan: Lagstiftning som kräver att leverantörer som erbjuder tillgång till offentliga kommunikationstjänster online och leverantörer av värdtjänster lagrar personuppgifter m.m. som rör dessa tjänster generellt och utan åtskillnad[22].
- Med hänvisning till rättigheterna enligt artikel 8 i stadgan: En avsaknad av grundläggande principer för dataskydd och datasäkerhet skulle även kunna inkräkta på kärnan i rättigheten[23].

3.1.3.3 Berättigat syfte

47. Som redan har förklarats i punkt 3.1.3 måste begränsningar av de grundläggande rättigheterna verkligen uppfylla mål av allmänt samhällsintresse som erkänns av Europeiska unionen eller tillgodose behovet att skydda andra personers rättigheter och friheter.

48. Unionen erkänner såväl de mål som anges i artikel 3 i fördraget om Europeiska unionen som andra intressen som skyddas av särskilda bestämmelser i fördragen[24], dvs. bland annat ett område med frihet, säkerhet och rättvisa samt förebyggande och bekämpande av brott. I sina förbindelser med resten av världen bör unionen bidra till fred och säkerhet samt till skydd av de mänskliga rättigheterna.

49. Behovet att skydda andra personers rättigheter och friheter avser rättigheter för personer som skyddas av Europeiska unionens eller medlemsstaternas lagstiftning. Bedömningen måste göras i syfte att samordna kraven på skydd av respektive rättigheter och att skapa en rimlig jämvikt mellan dem[25].

3.1.3.4 Prövning av nödvändighet och proportionalitet

50. Om det är fråga om intrång i de grundläggande rättigheterna kan lagstiftarens utrymme för skönsmässig bedömning visa sig vara begränsat, både på nationell nivå och EU-nivå. Detta beror på ett antal omständigheter, såsom bland annat det område som berörs, beskaffenheten av den rättighet som garanteras genom stadgan, ingreppets beskaffenhet och allvar samt ingreppets syfte[26]. Lagstiftningsåtgärderna måste vara lämpliga för att uppnå de legitima mål som eftersträvas med den berörda lagstiftningen. Åtgärderna får dessutom inte gå utöver vad som är lämpligt och nödvändigt för att uppnå dessa mål[27]. Ett mål av allmänt samhällsintresse kan inte, trots dess grundläggande betydelse, i sig ensamt motivera en begränsning av en grundläggande rättighet[28].

51. Enligt EU-domstolens fasta rättspraxis ska undantag från och begränsningar av skyddet för personuppgifter inskränkas till vad som är strängt nödvändigt[29]. Detta förutsätter även att det inte

---

[21] Europeiska unionens domstol, C-203/15 – Tele2 Sverige, punkt 101 med hänvisning till EU-domstolen, C-293/12 och C-594/12, punkt 39.
[22] Europeiska unionens domstol, C-512/18, La Quadrature du Net, punkt 209 och följande.
[23] Europeiska unionens domstol, C-594/12, punkt 40.
[24] Förklaringar avseende stadgan om de grundläggande rättigheterna, Avdelning I, Förklaring till artikel 52, EUT C 303, 14.12.2007, s. 17.
[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Art. 52 Rn. 31–32.
[26] Europeiska unionens domstol, C-594/12, punkt 47 med följande källor: se, analogt beträffande artikel 8 i Europakonventionen Europadomstolens dom i målet S. och Marper mot Förenade kungariket [GC], nr 30562/04 och 30566/04, punkt 102, ECHR 2008-V.
[27] Europeiska unionens domstol, C-594/12, punkt 46 med följande källor: mål C-343/09 Afton Chemical EU:C:2010:419, punkt 45, Volker und Markus Schecke och Eifert EU:C:2010:662, punkt 74, målen C-581/10 och C-629/10 Nelson m.fl. EU:C:2012:657, punkt 71, mål C-283/11 Sky Österreich EU:C:2013:28, punkt 50 samt mål C-101/12 Schaible EU:C:2013:661, punkt 29.
[28] Europeiska unionens domstol, C-594/12, punkt 51.
[29] Europeiska unionens domstol, C-594/12, punkt 52, med följande källor: mål C-473/12 IPI EU:C:2013:715, punkt 39 och där angiven rättspraxis.

finns några mindre integritetskränkande sätt att uppnå syftet. Möjliga alternativ, som – beroende på syftet – kan innefatta ytterligare personal, mer omfattande polisarbete eller ytterligare gatubelysning, måste identifieras och bedömas noggrant. Lagstiftningsåtgärder bör göra åtskillnader och vara inriktade på de personer som omfattas av dem mot bakgrund av syftet, t.ex. att bekämpa allvarliga brott. Om åtgärderna generellt omfattar samtliga personer utan sådana åtskillnader, begränsningar eller undantag förstärker de intrånget[30]. Intrånget förstärks även om behandlingen av uppgifter omfattar en betydande del av befolkningen[31].

52. Skyddet för personuppgifter, vilket följer av den uttryckliga skyldigheten i artikel 8.1 i stadgan, är av särskild betydelse för rätten till respekt för privatlivet i artikel 7 i stadgan[32]. Lagstiftningen måste föreskriva tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av den aktuella åtgärden och som slår fast skyddsåtgärder, så att de personer vilkas uppgifter har behandlats har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk och otillåten tillgång eller användning[33]. Nödvändigheten av sådana skyddsåtgärder är av än större betydelse när personuppgifterna är föremål för automatisk behandling och risken för otillåten tillgång till uppgifterna är stor[34]. Dessutom kan interna eller externa (t.ex. rättsliga) tillstånd för införande av ansiktsigenkänningsteknik fungera som skyddsåtgärder, vilket kan visa sig vara nödvändigt i vissa fall där intrången är allvarliga[35].

53. De fastställda reglerna måste anpassas till den specifika situationen, t.ex. mängden av behandlade uppgifter, uppgifternas art[36]och risken för otillåten åtkomst till uppgifterna. Detta kräver regler som på ett tydligt och strängt sätt skulle reglera skyddet av uppgifterna och deras säkerhet i syfte att säkerställa fullständig integritet och konfidentialitet för uppgifterna[37].

54. När det gäller förhållandet mellan personuppgiftsansvariga och personuppgiftsbiträden bör det inte vara tillåtet för personuppgiftsbiträden att endast ta hänsyn till ekonomiska överväganden vid bestämmandet av den säkerhetsnivå som de ska tillämpa på personuppgifterna, eftersom detta skulle kunna leda till en lägre skyddsnivå[38].

55. En rättsakt måste innehålla materiella och formella villkor samt objektiva kriterier för att avgränsa behöriga myndigheters tillgång till uppgifterna och deras senare användning. För utredning, avslöjande och åtal av brott måste brotten anses vara tillräckligt allvarliga för att motivera det omfattande och allvarliga ingreppet i de grundläggande rättigheterna i exempelvis artiklarna 7 och 8 i stadgan[39].

56. Uppgifterna måste behandlas på ett sätt som säkerställer tillämpligheten och effekterna av EU:s dataskyddsregler, särskilt de som föreskrivs i artikel 8 i stadgan, där det anges att en oberoende

[30] Europeiska unionens domstol, C-594/12, punkt 57.
[31] Europeiska unionens domstol, C-594/12, punkt 56.
[32] Europeiska unionens domstol, C-594/12, punkt 53.
[33] Europeiska unionens domstol, C-594/12, punkt 54, med följande källor: se, analogt beträffande artikel 8 i Europakonventionen, Europadomstolens dom av den 1 juli 2008 i målet Liberty m.fl. mot Förenade kungariket, nr 58243/00, punkterna 62 och 63, Rotaru mot Rumänien, punkterna 57–59 samt S. och Marper mot Förenade kungariket, punkt 99.
[34] Europeiska unionens domstol, C-594/12, punkt 55, med följande källor: se, analogt beträffande artikel 8 i Europakonventionen, Europadomstolens dom i målet S. och Marper mot Förenade kungariket, punkt 103 och av den 18 april 2013 i målet M. K. mot Frankrike, nr 19522/09, punkt 35.
[35] Europeiska domstolen för de mänskliga rättigheterna, Szabó och Vissy mot Ungern, punkterna 73–77.
[36] Se även de skärpta kraven på tekniska och organisatoriska åtgärder vid behandling av särskilda kategorier av uppgifter, artikel 29.1 i brottsdatadirektivet.
[37] Europeiska unionens domstol, C-594/12, punkt 66.
[38] Europeiska unionens domstol, C-594/12, punkt 67.
[39] Europeiska unionens domstol, C-594/12, punkterna 60 och 61.

myndighet ska kontrollera att skydds- och säkerhetskraven följs. Den geografiska plats där behandlingen äger rum kan vara relevant i en sådan situation[40].

57. När det gäller de olika stegen i behandlingen av personuppgifter bör åtskillnad göras mellan kategorierna av uppgifter utifrån deras nytta för det mål som eftersträvas eller utifrån de personer som berörs[41]. Villkoren för behandlingen, till exempel lagringstiden, måste bestämmas enligt objektiva kriterier för att säkerställa att intrånget är begränsat till vad som är strängt nödvändigt[42].

58. I varje enskild situation måste bedömningen av nödvändighet och proportionalitet omfatta och ta hänsyn till alla konsekvenser som faller inom ramen för andra grundläggande rättigheter, däribland människans värdighet enligt artikel 1 i stadgan, tankefrihet, samvetsfrihet och religionsfrihet enligt artikel 10 i stadgan, yttrandefrihet enligt artikel 11 i stadgan samt mötesfrihet och föreningsfrihet enligt artikel 12 i stadgan.

59. Dessutom måste det betraktas som ett allvarligt problem att behandlingen, om uppgifterna behandlas systematiskt utan de registrerades vetskap, sannolikt kommer att ge en allmän känsla av ständig övervakning[43]. Detta kan leda till avskräckande effekter med avseende på vissa eller alla de berörda grundläggande rättigheterna.

60. För att underlätta bedömningen av nödvändighet och proportionalitet i lagstiftningsåtgärder som rör ansiktsigenkänning inom brottsbekämpning skulle lagstiftarna både på nationell nivå och unionsnivå kunna dra nytta av de praktiska verktyg som tagits fram särskilt för denna uppgift. Framför allt skulle Europeiska datatillsynsmannens verktygslåda för nödvändighet och proportionalitet[44] kunna användas.

3.1.3.5 Artiklarna 52.3 och 53 i stadgan (skyddsnivå, även i förhållande till den europeiska konventionen om de mänskliga rättigheterna)

61. Enligt artiklarna 52.3 och 53 i stadgan ska innebörden och räckvidden av de rättigheter i stadgan som motsvarar de rättigheter som garanteras av den europeiska konventionen om de mänskliga rättigheterna vara desamma som de som fastställs i den konventionen. Artikel 7 i stadgan har en motsvarighet i konventionen, men detsamma gäller inte för artikel 8 i stadgan[45]. Artikel 52.3 i stadgan hindrar inte att ett mer omfattande skydd föreskrivs i unionsrätten. Eftersom den europeiska konventionen om de mänskliga rättigheterna inte utgör något rättsligt instrument som formellt införlivats med unionsrätten ska unionsrättsakter tolkas utifrån de grundläggande rättigheterna i stadgan[46].

62. Enligt artikel 8 i den europeiska konventionen om de mänskliga rättigheterna får en offentlig myndighet inte ingripa i utövandet av denna rätt till respekt för privat- och familjeliv annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter.

---

[40] Europeiska unionens domstol, C-594/12, punkt 68.
[41] Europeiska unionens domstol, C-594/12, punkt 63.
[42] Europeiska unionens domstol, C-594/12, punkt 64.
[43] Europeiska unionens domstol, C-594/12, punkt 37.
[44] Europeiska datatillsynsmannen: *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit* (inte översatt till svenska), 11 april 2017 och Europeiska datatillsynsmannen: *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (inte översatt till svenska), 19 december 2019.
[45] Europeiska unionens domstol, C-203/15, Tele2 Sverige, punkt 129.
[46] Europeiska unionens domstol, C-311/18, punkt 99.

63. I konventionen fastställs även normer för hur begränsningar får göras. Ett grundläggande krav, vid sidan av rättsstatsprincipen, är förutsägbarhet. För att uppfylla kravet om förutsägbarhet måste lagen vara tillräckligt tydlig, så att enskilda personer kan få tillräcklig kännedom om de omständigheter som måste råda för att myndigheterna ska ha rätt att tillgripa sådana åtgärder och vilka villkor som måste vara uppfyllda[47]. Detta krav erkänns av EU-domstolen och i EU:s dataskyddslagstiftning (se avsnitt 3.2.1.1).

64. För att ytterligare specificera rättigheterna i artikel 8 i den europeiska konventionen om de mänskliga rättigheterna måste bestämmelserna i konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter[48] också respekteras fullt ut. Hänsyn måste emellertid tas till att dessa bestämmelser endast utgör en minsta standard mot bakgrund av den rådande unionsrätten.

3.2 Särskild rättslig ram – brottsdatadirektivet

65. En viss ram för användningen av ansiktsigenkänningsteknik fastställs i brottsdatadirektivet. För det första definieras begreppet *biometriska uppgifter*[49] i artikel 3.13 i direktivet. Mer information finns i avsnitt 2.1 ovan. För det andra klargörs i artikel 8.2 att en behandling för att vara laglig – förutom att vara nödvändig för de ändamål som anges i artikel 1.1 i direktivet – ska regleras i nationell lagstiftning som åtminstone specificerar syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål. Ytterligare bestämmelser av särskild betydelse när det gäller biometriska uppgifter finns i artiklarna 10 och 11 i brottsdatadirektivet. artikel 10 måste läsas tillsammans med artikel 8 i brottsdatadirektivet[50]. De principer för behandling av personuppgifter som fastställs i artikel 4 i brottsdatadirektivet bör alltid följas och vara vägledande vid bedömningar av möjlig biometrisk behandling via ansiktsigenkänning.

3.2.1 Behandling av särskilda kategorier av uppgifter för brottsbekämpande ändamål

66. Enligt artikel 10 i brottsdatadirektivet ska behandling av särskilda kategorier av uppgifter, däribland biometriska uppgifter, vara tillåten endast om det är absolut nödvändigt och under förutsättning att det finns lämpliga skyddsåtgärder för den registrerades rättigheter och friheter. Behandlingen måste dessutom vara tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, syfta till att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan fysisk person eller röra uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade. Denna allmänna klausul understryker hur känslig behandlingen av särskilda kategorier av uppgifter är.

3.2.1.1 Tillstånd enligt unionsrätten eller medlemsstaternas nationella rätt

67. Vad gäller den nödvändiga typen av lagstiftningsåtgärd anges följande i skäl 33 i brottsdatadirektivet: ”När det i detta direktiv hänvisas till medlemsstaternas nationella rätt, en rättslig grund eller

[47] Europeiska domstolen för de mänskliga rättigheterna, Dom i målet Copland mot Förenade kungariket, 3.4.2007, ansökan nr 62617/00, punkt 46.

[48] Europarådets fördragsserie nr 108.

[49] artikel 3.13 i brottsdatadirektivet: ”*biometriska uppgifter*: personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar [en] unik identifiering av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter.”

[50] WP258, Yttrande om vissa centrala frågor gällande direktivet om brottsbekämpning (EU 2016/680), s. 7.

lagstiftningsåtgärd innebär detta inte nödvändigtvis en lagstiftningsakt antagen av ett parlament, med förbehåll för krav i den berörda medlemsstatens konstitutionella ordning."[51]

68. Enligt artikel 52.1 i stadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan "vara föreskriven i lag". Detta motsvarar uttrycket "med stöd av lag" i artikel 8.2 i den europeiska konventionen om de mänskliga rättigheterna, vilket inte bara innebär överensstämmelse med tillämplig lagstiftning, utan även rör lagens kvalitet utan att det påverkar aktens art, dvs. lagen ska vara förenlig med rättsstatsprincipen.

69. Vidare anges följande i skäl 33 i brottsdatadirektivet: "Medlemsstaternas nationella rätt, den rättsliga grunden eller lagstiftningsåtgärden bör emellertid i dessa fall vara tydlig och precis, och dess tillämpning förutsägbar för dem som omfattas av den i enlighet med rättspraxis från domstolen och Europeiska domstolen för de mänskliga rättigheterna. Medlemsstaternas nationella rätt som reglerar behandlingen av personuppgifter inom tillämpningsområdet för detta direktiv bör åtminstone specificera målen, vilka personuppgifter som ska behandlas, behandlingens ändamål, förfarandena för att bevara personuppgifternas integritet och konfidentialitet samt förfarandena för förstöring av dem […]."

70. Den nationella lagstiftningen måste vara tillräckligt tydlig för att ge de registrerade kännedom om de omständigheter och villkor under vilka personuppgiftsansvariga har rätt att tillgripa sådana åtgärder. Detta inbegriper möjliga förutsättningar för behandlingen, till exempel särskilda typer av bevis eller behovet av rättsligt eller internt tillstånd. Den respektive lagstiftningen kan vara teknikneutral i den mån de specifika riskerna och egenskaperna hos den behandling av personuppgifter som utförs med system för ansiktsigenkänning hanteras på ett tillfredsställande sätt. I linje med brottsdatadirektivet och rättspraxis från Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna måste lagstiftningsåtgärder som syftar till att tillhandahålla en rättslig grund för en åtgärd som bygger på användningen av ansiktsigenkänning vara förutsägbara för de registrerade.

71. En lagstiftningsåtgärd som endast utgör ett införlivande av den allmänna klausulen i artikel 10 i brottsdatadirektivet kan inte åberopas som en lag som tillåter behandlingen av biometriska uppgifter med hjälp av ansiktsigenkänningsteknik för brottsbekämpande ändamål.

72. Förutom biometriska uppgifter reglerar artikel 10 i brottsdatadirektivet även behandlingen av andra särskilda kategorier av uppgifter, däribland sexuell läggning, politiska åsikter och religiösa övertygelser, och är således mycket omfattande. Dessutom skulle en sådan bestämmelse sakna särskilda krav som anger under vilka omständigheter och på vilka villkor de brottsbekämpande myndigheterna skulle ha rätt att använda ansiktsigenkänningsteknik. På grund av hänvisningen till andra typer av uppgifter och det uttryckliga behovet av särskilda skyddsåtgärder utan ytterligare specifikationer kan den nationella bestämmelse varigenom artikel 10 i brottsdatadirektivet införlivas i nationell rätt – med en liknande allmän och abstrakt formulering – inte åberopas som rättslig grund för behandling av biometriska uppgifter som inbegriper ansiktsigenkänning, eftersom den skulle sakna precision och förutsägbarhet. I enlighet med artikel 28.2 eller artikel 46.1 c i brottsdatadirektivet bör den nationella tillsynsmyndigheten för dataskydd rådfrågas innan lagstiftaren skapar en ny rättslig grund för behandling av biometriska uppgifter med hjälp av ansiktsigenkänning.

[51] Den typ av lagstiftningsåtgärder som övervägs måste följa unionsrätten eller den nationella lagstiftningen. Beroende på begränsningens grad av intrång kan en särskild lagstiftningsåtgärd, med beaktande av normnivån, krävas på nationell nivå.

3.2.1.2 Absolut nödvändigt

73. Behandlingen kan endast betraktas som ”absolut nödvändig” om intrånget i skyddet av personuppgifter och dess begränsningar begränsas till vad som är absolut nödvändigt[52]. Med tillägget av bestämningen ”absolut” avsåg lagstiftaren att särskilda kategorier av uppgifter endast skulle behandlas under villkor som var ännu striktare än villkoren för nödvändighet (se ovan, punkt 3.1.3.4). Detta krav bör tolkas som ofrånkomligt. Det begränsar den brottsbekämpande myndighetens bedömningsmarginal vid nödvändighetsprövningen till ett absolut minimum. I enlighet med EU-domstolens fasta rättspraxis är villkoret ”absolut nödvändighet” även nära kopplat till kravet på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behandling får ske, vilket utesluter all behandling av allmän eller systematisk karaktär[53].

3.2.1.3 Offentliggjord på ett tydligt sätt

74. Vid bedömningen av om behandlingen avser uppgifter som på ett tydligt sätt har offentliggjorts av den registrerade bör det erinras om att ett foto som sådant inte systematiskt betraktas som biometriska uppgifter[54]. Det faktum att ett fotografi har offentliggjorts på ett tydligt sätt av den registrerade innebär därför inte att de biometriska uppgifter som kan hämtas från fotografiet med särskilda tekniska medel anses ha offentliggjorts på ett tydligt sätt.

75. När det gäller personuppgifter i allmänhet måste den registrerade avsiktligt ha gjort den biometriska mallen (och inte bara en ansiktsbild) fritt tillgänglig och offentlig genom en öppen källa för att de biometriska uppgifterna ska anses vara offentliggjorda på ett tydligt sätt. Om en tredje part lämnar ut de biometriska uppgifterna kan uppgifterna inte anses ha offentliggjorts på ett tydligt sätt av den registrerade.

76. Dessutom räcker det inte med att tolka den registrerades beteende för att anse att biometriska uppgifter har offentliggjorts på ett tydligt sätt. När det till exempel gäller sociala nätverk eller onlineplattformar anser EDPB att det faktum att den registrerade inte har aktiverat eller ställt in några särskilda sekretessfunktioner inte är tillräckligt för att anse att den registrerade har offentliggjort sina personuppgifter på ett tydligt sätt och att dessa uppgifter (t.ex. foton) kan behandlas i biometriska mallar och användas för identifieringsändamål utan den registrerades samtycke. Mer allmänt bör standardinställningarna för en tjänst, t.ex. att mallar görs allmänt tillgängliga eller att det inte finns några valmöjligheter, dvs. att mallarna offentliggörs utan att användaren kan ändra inställningarna, inte på något sätt tolkas som att uppgifterna har offentliggjorts på ett tydligt sätt.

3.2.2 Automatiserat individuellt beslutsfattande, inbegripet profilering

77. I artikel 11.1 i brottsdatadirektivet föreskrivs att medlemsstaterna generellt ska förbjuda beslut som enbart grundas på automatiserad behandling, inbegripet profilering, som har negativa rättsliga följder för den registrerade eller i betydande grad påverkar honom eller henne. Som ett undantag från detta allmänna förbud kan en sådan behandling vara möjlig om den är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt som den personuppgiftsansvarige lyder under och som föreskriver lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, åtminstone rätten till mänskligt

[52] Samstämmig rättspraxis om den grundläggande rätten till respekt för privatlivet, se EU-domstolens domar i målen C-73/07, punkt 56 (Satakunnan Markkinapörssi och Satamedia), C-92/09 och C-93/09, punkt 77 (Schecke och Eifert), C-594/12, punkt 52 (Digital Rights) och C-362/14, punkt 92 (Schrems).

[53] Europeiska unionens domstols dom i mål C-623/17, punkt 78.

[54] Se skäl 51 i den allmänna dataskyddsförordningen: ”Behandling av foton bör inte systematiskt anses utgöra behandling av särskilda kategorier av personuppgifter, eftersom foton endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person.”

ingripande från den personuppgiftsansvariges sida. Behandlingen får endast användas restriktivt. Denna tröskel gäller för ordinarie (dvs. inte särskilda) kategorier av personuppgifter. En ännu högre tröskel och en mer restriktiv användning gäller för undantaget enligt artikel 11.2 i brottsdatadirektivet. Där betonas att beslut enligt den första punkten i artikeln inte får grundas på särskilda kategorier av uppgifter, dvs. i synnerhet biometriska uppgifter, för att unikt identifiera en fysisk person. Ett undantag får endast beviljas om lämpliga åtgärder har vidtagits för att skydda den registrerades rättigheter och friheter och den berörda fysiska personens berättigade intressen. Detta undantag ska tolkas som komplement till och mot bakgrund av förutsättningarna i artikel 10 i brottsdatadirektivet.

78. Beroende på systemet för ansiktsigenkänning är det inte alltid säkert att mänskligt ingripande vid bedömningen av resultaten i sig utgör en tillräcklig garanti för respekten för enskildas rättigheter, och särskilt rätten till skydd av personuppgifter, med tanke på den möjliga snedvridning och de fel som kan uppstå till följd av själva behandlingen. Vidare kan mänskligt ingripande endast betraktas som en skyddsåtgärd om den person som ingriper kan ifrågasätta resultaten av ansiktsigenkänningen på ett kritiskt sätt. Det är mycket viktigt att personen förstår ansiktsigenkänningssystemet och dess begränsningar och kan tolka resultaten korrekt. Det är även nödvändigt att inrätta en arbetsplats och en organisation som motverkar effekterna av automationssnedvridning och inte främjar ett okritiskt godtagande av resultaten, t.ex. på grund av tidspress, betungande förfaranden och möjliga negativa effekter på karriären.

79. Enligt artikel 11.3 i brottsdatadirektivet ska profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter, däribland biometriska uppgifter, förbjudas i enlighet med unionsrätten. Enligt artikel 3.4 i brottsdatadirektivet avses med *profilering* varje form av automatiserad behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar. Vid en bedömning av vilka åtgärder som är lämpliga för att skydda den registrerades rättigheter och friheter och den berörda fysiska personens berättigade intressen är det viktigt att komma ihåg att användningen av ansiktsigenkänningsteknik kan leda till profilering beroende på hur och för vilket ändamål tekniken tillämpas. Under alla omständigheter ska profilering som leder till diskriminering av fysiska personer på grundval av särskilda kategorier av personuppgifter vara förbjuden i enlighet med unionsrätten och artikel 11.3 i brottsdatadirektivet.

3.2.3 Kategorier av registrerade

80. I artikel 6 i brottsdatadirektivet fastställs behovet av att skilja mellan olika kategorier av registrerade. Denna åtskillnad ska göras i tillämpliga fall och så långt det är möjligt. Den måste påverka det sätt som uppgifterna behandlas på. Av de exempel som ges i artikel 6 i brottsdatadirektivet kan man dra slutsatsen att behandlingen av personuppgifter i regel måste uppfylla kriterierna för nödvändighet och proportionalitet även med avseende på kategorin av registrerade[55]. Exemplen visar även att ett intrång med största sannolikhet inte är motiverat när det gäller registrerade beträffande vilka det inte föreligger något indicium som ger anledning att tro att deras beteende ens kan ha ett indirekt och avlägset samband med det berättigade syftet enligt brottsdatadirektivet[56]. Om ingen åtskillnad enligt artikel 6 i brottsdatadirektivet är tillämplig eller möjlig måste undantaget från regeln i artikel 6 i det direktivet noggrant beaktas vid bedömningen av intrångets nödvändighet och proportionalitet. Åtskillnaden mellan olika kategorier av registrerade framstår som ett väsentligt krav när det gäller

[55] Se även Europeiska unionens domstol, C-594/12, punkterna 56–59.
[56] Se även Europeiska unionens domstol, C-594/12, punkt 58.

behandling av personuppgifter som inbegriper ansiktsigenkänning, även med tanke på möjliga falska positiva eller falska negativa resultat som kan få betydande konsekvenser för de registrerade vid en utredning.

81. Som redan nämnts måste bestämmelserna i stadgan respekteras vid genomförande av unionsrätten (se artikel 52 i stadgan). Den ram och de kriterier som föreskrivs i brottsdatadirektivet ska därför läsas mot bakgrund av stadgan. Unionens och medlemsstaternas rättsakter får inte vara mindre genomgripande än denna åtgärd, utan måste säkerställa stadgans fulla verkan.

3.2.4 Den registrerades rättigheter

82. EDPB har redan gett vägledning om registrerades rättigheter i olika situationer enligt den allmänna dataskyddsförordningen[57]. Liknande rättigheter för registrerade föreskrivs i brottsdatadirektivet, och allmän vägledning har lämnats i ett yttrande från artikel 29-arbetsgruppen, som har godkänts av EDPB[58]. Under vissa omständigheter ger brottsdatadirektivet utrymme för begränsningar av dessa rättigheter. Parametrarna för dessa begränsningar kommer att beskrivas närmare i avsnitt 3.2.4.6, ”Berättigade begränsningar av den registrerades rättigheter”.

83. De rättigheter för registrerade som anges i kapitel III i brottsdatadirektivet gäller naturligtvis även vid behandling av personuppgifter via ansiktsigenkänningsteknik. Följande kapitel är inriktat på några av de rättigheter och aspekter som kan vara av särskilt intresse. I detta kapitel och dess analys förutsätts att den aktuella behandlingen med ansiktsigenkänningsteknik uppfyller de rättsliga krav som beskrivs i föregående kapitel.

84. Eftersom behandling av personuppgifter via ansiktsigenkänningsteknik har en särskild karaktär (behandling av särskilda kategorier av personuppgifter utan någon uppenbar interaktion med den registrerade) måste den personuppgiftsansvarige noggrant överväga hur (eller om) kraven i brottsdatadirektivet kan uppfyllas innan behandlingen inleds. Framför allt måste den personuppgiftsansvarige noggrant analysera

- vilka de registrerade är (ofta omfattas fler personer än den eller de personer som utgör den huvudsakliga målgruppen för behandlingen),
- hur de registrerade får information om behandlingen med ansiktsigenkänningsteknik (se avsnitt 3.2.4.1),
- hur de registrerade kan utöva sina rättigheter (här kan såväl rätten till information och tillgång som rätten till rättelse eller begränsning vara särskilt svår att upprätthålla om ansiktsigenkänningsteknik används i alla andra fall än ”en mot en”-verifiering i direkt kontakt med den registrerade).

3.2.4.1 Information om de registrerades rättigheter i en koncis, begriplig och lättillgänglig form

85. En av utmaningarna vid användning av ansiktsigenkänningsteknik är att säkerställa att de registrerade får information om att deras biometriska uppgifter behandlas. Detta är särskilt komplicerat för en brottsbekämpande myndighet som använder ansiktsigenkänningsteknik för att analysera videomaterial som härrör från eller tillhandahålls av tredje part, eftersom myndigheten i regel inte kan meddela den registrerade vid insamlingstillfället (t.ex. via en skylt på plats). Allt videomaterial som inte är relevant för utredningen (eller behandlingens ändamål) bör alltid raderas eller anonymiseras (t.ex. genom att sudda ut vissa delar så att de inte kan återskapas i efterhand) innan biometriska uppgifter

[57] Se till exempel EDPB, *Guidelines 01/2022 on data subject’s rights – Right of access* (inte översatt till svenska) och EDPB:s riktlinjer 3/2019 för behandling av personuppgifter genom videoenheter.
[58] WP258, Yttrande om vissa centrala frågor gällande direktivet om brottsbekämpning (EU 2016/680).

behandlas, för att säkerställa att minimeringsprincipen i artikel 4.1 e i brottsdatadirektivet och informationsskyldigheterna i artikel 13.2 i brottsdatadirektivet har uppfyllts. Det är den personuppgiftsansvariges ansvar att bedöma vilken information som kan vara av betydelse för den registrerade när han eller hon utövar sina rättigheter och att se till att nödvändig information tillhandahålls. För att den registrerade ska kunna utöva sina rättigheter på ett effektivt sätt måste den personuppgiftsansvarige uppfylla sina informationsskyldigheter.

86. I artikel 13.1 i brottsdatadirektivet anges vilken information som i vanliga fall ska lämnas till den registrerade. Denna information kan tillhandahållas via den personuppgiftsansvariges webbplats, i tryckt form (t.ex. en broschyr som finns tillgänglig på begäran) eller via andra källor som är lätta att komma åt för den registrerade. Den personuppgiftsansvarige ska under alla omständigheter se till att följande information tillhandahålls:

- Den personuppgiftsansvariges och dataskyddsombudets uppgifter, inklusive kontaktuppgifter.
- Behandlingens ändamål och att uppgifterna behandlas via ansiktsigenkänning.
- Rätten att lämna in ett klagomål till en tillsynsmyndighet samt tillsynsmyndighetens kontaktuppgifter.
- Rätten att begära tillgång till och rättelse eller radering av personuppgifter och begränsning av behandlingen av personuppgifter.

87. I specifika fall, enligt nationell lagstiftning som bör överensstämma med artikel 13.2 i brottsdatadirektivet[59], t.ex. vid behandling via ansiktsigenkänning, måste dessutom följande information lämnas direkt till den registrerade:

- Behandlingens rättsliga grund.
- Information om var personuppgifterna samlades in utan den registrerades vetskap.
- Den period under vilken personuppgifterna kommer att lagras eller, om det inte är möjligt, de kriterier som används för att fastställa denna period.
- I tillämpliga fall, kategorierna av mottagare av personuppgifterna (inbegripet tredjeländer eller internationella organisationer).

88. Artikel 13.1 i brottsdatadirektivet handlar om allmän information som ska göras tillgänglig för allmänheten, medan artikel 13.2 i samma direktiv handlar om information som ska lämnas utöver denna information till en viss registrerad i specifika fall, till exempel när data samlas in direkt från den registrerade, eller indirekt utan den registrerades kännedom[60]. Det finns inte någon tydlig definition av vad som avses med ”specifika fall” i artikel 13.2 i brottsdatadirektivet. I direktivet hänvisas emellertid till situationer där de registrerade måste göras medvetna om den behandling som gäller dem specifikt och få lämplig information för att kunna utöva sina rättigheter på ett effektivt sätt. EDPB anser att flera faktorer måste beaktas vid bedömningen av huruvida ett ”specifikt fall” föreligger, däribland om personuppgifter samlas in utan den registrerades vetskap, eftersom detta skulle vara det enda sättet att göra det möjligt för registrerade att effektivt utöva sina rättigheter. Andra exempel på ”specifika fall” skulle kunna vara om personuppgifter behandlas vidare i samband med ett internationellt straffrättsligt samarbetsförfarande eller i situationer där personuppgifter behandlas vid

[59] T.ex. avsnitt 56.1 i den tyska federala dataskyddslagen, där det bland annat anges vilken information som måste lämnas till registrerade i samband med infiltrationsverksamhet.
[60] WP258 Yttrande om vissa centrala frågor gällande direktivet om brottsbekämpning (EU 2016/680), s. 18.

hemliga utredningar i enlighet med nationell lagstiftning. Dessutom följer det av skäl 38 i brottsdatadirektivet att de registrerade måste informeras om alla steg i det automatiserade beslutsfattandet om beslutsfattandet uteslutande grundas på ansiktsigenkänning. Detta skulle även tyda på att det rör sig om ett specifikt fall där ytterligare information bör lämnas till den registrerade i enlighet med artikel 13.2 i brottsdatadirektivet[61].

89. Slutligen bör det noteras att medlemsstaterna enligt artikel 13.3 i direktivet får anta lagstiftningsåtgärder som begränsar skyldigheten att tillhandahålla information i specifika fall och för vissa ändamål. Detta gäller i den utsträckning och så länge som en sådan åtgärd är nödvändig och proportionell i ett demokratiskt samhälle med hänsyn tagen till den registrerades grundläggande rättigheter och berättigade intressen.

3.2.4.2 Rätten till tillgång

90. I regel har den registrerade rätt att få en positiv eller negativ bekräftelse på all behandling av hans eller hennes personuppgifter och, om svaret är positivt, tillgång till personuppgifterna som sådana, plus ytterligare information, enligt förteckningen i artikel 14 i brottsdatadirektivet. Vid användning av ansiktsigenkänningsteknik, i fall där biometriska uppgifter även lagras och kopplas till en identitet med alfanumeriska uppgifter, bör den behöriga myndigheten ha möjlighet att godkänna en begäran om tillgång på grundval av en sökning med dessa alfanumeriska uppgifter utan någon ytterligare behandling av andras biometriska uppgifter (dvs. sökning med ansiktsigenkänningsteknik i en databas). Principen om uppgiftsminimering ska följas, och inga andra uppgifter än de som är nödvändiga för behandlingens ändamål bör lagras.

3.2.4.3 Rätten till rättelse av personuppgifter

91. Eftersom tekniken för ansiktsigenkänning har vissa brister är det särskilt viktigt att personuppgiftsansvariga tillgodoser begäranden om rättelse av personuppgifter. Detta kan även vara fallet om en registrerad på grundval av ansiktsigenkänningsteknik har placerats i en felaktig kategori, t.ex. i kategorin ”misstänkta” på grundval av ett första antagande om personens beteende i en videofilm. Riskerna för de registrerade är särskilt allvarliga om sådana felaktiga uppgifter lagras i en polisdatabas och/eller delas med andra enheter. Den personuppgiftsansvarige måste korrigera lagrade uppgifter och system för ansiktsigenkänningsteknik i enlighet med detta (se skäl 47 i brottsdatadirektivet).

3.2.4.4 Rätten till radering

92. Ansiktsigenkänningsteknik kommer i de flesta fall – såvida den inte används för ”en mot en”-verifiering/autentisering – att omfatta biometriska uppgifter om ett stort antal registrerade. Det är därför viktigt att den personuppgiftsansvarige i förväg överväger var gränserna för behandlingens ändamål och nödvändighet ska gå, så att en begäran om radering i enlighet med artikel 16 i brottsdatadirektivet kan hanteras utan onödigt dröjsmål (eftersom den personuppgiftsansvarige bland annat måste radera personuppgifter som behandlas utöver vad den tillämpliga lagstiftningen tillåter enligt artiklarna 4, 8 och 10 i brottsdatadirektivet).

3.2.4.5 Rätten till begränsning

93. Om den registrerade bestrider uppgifternas riktighet och uppgifternas riktighet inte kan fastställas (eller om personuppgifterna måste sparas för framtida bevisning) är den personuppgiftsansvarige skyldig att begränsa behandlingen av den registrerades personuppgifter i enlighet med artikel 16 i

[61] Notera skillnaden mellan ”göras tillgänglig för […] den registrerade” i artikel 13.1 i brottsdatadirektivet och ”lämna […] till den registrerade” i artikel 13.2 i samma direktiv. Enligt artikel 13.2 i brottsdatadirektivet måste den personuppgiftsansvarige säkerställa att informationen når den registrerade om det inte är tillräckligt att offentliggöra informationen på en webbplats.

brottsdatadirektivet. Detta blir särskilt viktigt när det gäller ansiktsigenkänningsteknik (som baseras på algoritmer och därmed aldrig visar ett slutgiltigt resultat) i situationer där stora mängder uppgifter samlas in och där identifieringens noggrannhet och kvalitet kan variera. Om videomaterialet är av dålig kvalitet (t.ex. filmer från en brottsplats) ökar risken för falska positiva resultat. Dessutom ökar risken för falska positiva eller falska negativa resultat om ansiktsbilderna i en bevakningslista inte uppdateras regelbundet. I vissa fall, där uppgifterna inte kan raderas på grund av att det finns rimliga skäl att anta att en radering skulle kunna påverka den registrerades berättigade intressen, bör uppgifterna i stället begränsas och endast behandlas för det ändamål som hindrade att de raderades (se skäl 47 i brottsdatadirektivet).

3.2.4.6 Berättigade begränsningar av den registrerades rättigheter

94. När det gäller den personuppgiftsansvariges informationsskyldigheter och de registrerades rätt till tillgång tillåts begränsningar endast om de fastställs i lagstiftningen, vilken i sin tur måste utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen (se artiklarna 13.3, 13.4, 15 och 16.4 i brottsdatadirektivet). När ansiktsigenkänningsteknik används för brottsbekämpning kan man förvänta sig att den kommer att användas under omständigheter där det skulle vara skadligt för det eftersträvade syftet att informera den registrerade eller ge den registrerade tillgång till uppgifterna. Detta kan till exempel vara fallet vid en polisutredning av ett brott eller i en situation där den nationella eller allmänna säkerheten måste skyddas.

95. Rätten till tillgång innebär inte automatiskt tillgång till all information, t.ex. i ett straffrättsligt ärende där den registrerades personuppgifter förekommer. Ett bra exempel på när begränsningar av rätten kan tillåtas skulle kunna vara vid en brottsutredning.

3.2.4.7 Utövande av rättigheter genom tillsynsmyndigheten

96. I fall där begränsningar av utövandet av rättigheter är berättigade enligt kapitel III i brottsdatadirektivet kan den registrerade begära att dataskyddsmyndigheten utövar den registrerades rättigheter genom att kontrollera lagligheten i den personuppgiftsansvariges behandling. Det är den personuppgiftsansvariges ansvar att underrätta den registrerade om möjligheten att utöva sina rättigheter på detta sätt (se artiklarna 17 och 46.1 g i brottsdatadirektivet). Vid användning av ansiktsigenkänningsteknik innebär detta att den personuppgiftsansvarige måste se till att lämpliga åtgärder vidtas så att en sådan begäran kan hanteras, t.ex. genom att möjliggöra sökning i registrerat material, förutsatt att den registrerade tillhandahåller tillräcklig information för att lokalisera hans eller hennes personuppgifter.

3.2.5 Andra rättsliga krav och skyddsåtgärder

3.2.5.1 Artikel 27 Konsekvensbedömning avseende dataskydd

97. En konsekvensbedömning avseende dataskydd är ett obligatoriskt krav innan ansiktsigenkänningsteknik får användas eftersom typen av behandling, särskilt med ny teknik, och behandlingens art, omfattning, sammanhang och ändamål sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter. Eftersom användningen av ansiktsigenkänningsteknik innebär en systematisk automatisk behandling av särskilda kategorier av uppgifter är det i regel den personuppgiftsansvarige som ska genomföra en konsekvensbedömning avseende dataskydd. Konsekvensbedömningen bör åtminstone innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av behandlingens nödvändighet och proportionalitet i förhållande till ändamålen, en bedömning av riskerna för de registrerades rättigheter och friheter, de åtgärder som planeras för att hantera dessa risker, skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att påvisa efterlevnad. I syfte att öka förtroendet och öppenheten

rekommenderar EDPB att resultaten av sådana bedömningar, eller åtminstone de viktigaste resultaten och slutsatserna, offentliggörs[62].

3.2.5.2 Artikel 28 Förhandssamråd med tillsynsmyndigheten

98. Enligt artikel 28 i brottsdatadirektivet ska den personuppgiftsansvarige eller personuppgiftsbiträdet samråda med tillsynsmyndigheten före behandlingen av personuppgifter, om a) en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken, eller om b) typen av behandling, särskilt vid användning av ny teknik eller nya rutiner eller förfaranden, medför en hög risk för de registrerades rättigheter och friheter. Som redan förklarats i avsnitt 2.3 i dessa riktlinjer anser EDPB att införandet och användningen av ansiktsigenkänningsteknik i de flesta fall medför en hög risk för de registrerades rättigheter och friheter. Förutom en konsekvensbedömning avseende dataskydd bör därför den myndighet som inför tekniken samråda med den behöriga tillsynsmyndigheten innan systemet tas i bruk.

3.2.5.3 Artikel 29 Säkerhet i samband med behandling

99. De biometriska uppgifternas unika karaktär gör att den registrerade inte kan ändra dem om de skulle äventyras, t.ex. till följd av ett dataintrång. Den behöriga myndighet som inför och/eller använder ansiktsigenkänningsteknik bör därför vara särskilt uppmärksam på säkerheten i samband med behandlingen i enlighet med artikel 29 i brottsdatadirektivet. Framför allt bör den brottsbekämpande myndigheten säkerställa att systemet uppfyller relevanta standarder och vidta åtgärder för att skydda de biometriska mallarna[63]. Denna skyldighet är ännu mer relevant om den brottsbekämpande myndigheten använder en tredjepartsleverantör (som personuppgiftsbiträde).

3.2.5.4 Artikel 20 Inbyggt dataskydd och dataskydd som standard

100. Inbyggt dataskydd och dataskydd som standard, i enlighet med artikel 20 i brottsdatadirektivet, syftar till att säkerställa att tekniken omfattas av dataskyddsprinciper och skyddsåtgärder, såsom uppgiftsminimering och lagringsbegränsning, genom lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering, redan innan behandlingen av personuppgifter inleds, och att de kommer att tillämpas under hela användningstiden. Med tanke på den stora inneboende risken för fysiska personers rättigheter och friheter bör valet av sådana åtgärder inte enbart bero på ekonomiska hänsyn[64], utan i stället syfta till att genomföra den senaste tekniken för dataskydd. På samma sätt måste en brottsbekämpande myndighet som har för avsikt att tillämpa och använda ansiktsigenkänningsteknik från externa leverantörer, till exempel i samband med upphandlingen, säkerställa att den teknik som bygger på principerna om inbyggt dataskydd och dataskydd som standard används[65]. Detta innebär även att insynen i teknikens funktion inte får begränsas genom hänvisningar till företagshemligheter eller immateriella rättigheter.

3.2.5.5 Artikel 25 Loggning

101. I brottsdatadirektivet föreskrivs olika metoder som den personuppgiftsansvarige och personuppgiftsbiträdet kan använda för att visa att behandlingen är tillåten och för att säkerställa uppgifternas integritet och säkerhet. I detta avseende är systemloggar ett mycket användbart verktyg och en viktig garanti för kontrollen av om behandlingen är tillåten, både internt (dvs. egenkontroll) och

---

[62] För mer information, se WP248 rev.01, *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk”*.

[63] Se till exempel ISO/IEC 24745 Informationsteknik – Säkerhetstekniker – Biometriskt informationsskydd.

[64] Se skäl 53 i brottsdatadirektivet.

[65] För mer information, se EDPB:s riktlinjer om inbyggt dataskydd och dataskydd som standard https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

av externa tillsynsmyndigheter, till exempel dataskyddsmyndigheterna. Enligt artikel 25 i brottsdatadirektivet ska loggar föras över åtminstone följande typer av behandlingar i automatiserade behandlingssystem: insamling, ändring, läsning, utlämning inbegripet överföringar, sammanförande och radering. Dessutom bör loggarna över läsning och utlämning göra det möjligt att fastställa motivering, datum och tidpunkt för sådan behandling och i möjligaste mån vem som har läst eller lämnat ut personuppgifter, samt vilka som har fått tillgång till personuppgifterna. När det gäller system för ansiktsigenkänning rekommenderas dessutom loggning av följande behandlingar (delvis utöver artikel 25 i brottsdatadirektivet):

- Ändringar av referensdatabasen (tillägg, radering eller uppdatering). Loggen bör innehålla en kopia av den relevanta (tillagda, raderade eller uppdaterade) bilden om det inte går att kontrollera lagligheten eller resultatet av behandlingen på annat sätt.

- Identifierings- eller verifieringsförsök, inbegripet resultat och konfidensgrad. Principen om strikt minimering bör följas, så att endast bildens identifierare från referensdatabasen och inte hela referensbilden sparas i loggarna. Loggning av inmatade biometriska uppgifter bör undvikas om det inte är nödvändigt (t.ex. endast vid matchning).

- Identiteten hos den användare som begärde identifierings- eller verifieringsförsöket.

- Alla personuppgifter som lagras i systemens loggar omfattas av strikta ändamålsbegränsningar (t.ex. revisioner) och bör inte användas för andra ändamål (t.ex. för att kunna utföra igenkänning/verifiering, inbegripet av en bild som har raderats från referensdatabaserna). Säkerhetsåtgärder bör vidtas för att säkerställa loggarnas integritet, och automatiska övervakningssystem för att upptäcka missbruk av loggarna rekommenderas starkt. Säkerhetsåtgärderna för referensdatabasens loggar bör vara likvärdiga med referensdatabasen när det gäller lagring av ansiktsbilder. Dessutom bör automatiska förfaranden införas för att säkerställa att loggarnas lagringsperioder inte överskrids.

3.2.5.6 Artikel 4.4 Ansvarsskyldighet

102. Den personuppgiftsansvarige måste kunna visa att behandlingen är förenlig med principerna i artikel 4.1–4.3 (se artikel 4.4 i brottsdatadirektivet). En systematisk och aktuell dokumentation av systemet (inbegripet uppdateringar, uppgraderingar och träning av algoritmer), de tekniska och organisatoriska åtgärderna (inbegripet övervakning av systemets prestanda och möjligt mänskligt ingripande) samt behandlingen av personuppgifter är avgörande i detta avseende. Enligt artikel 25 i brottsdatadirektivet är loggning ett särskilt viktigt steg för att visa att behandlingen är tillåten (se avsnitt 3.2.5.5). Principen om ansvarsskyldighet avser inte bara systemet och behandlingen, utan även dokumentationen av rättssäkerhetsgarantier, däribland nödvändighets- och proportionalitetsbedömningar, konsekvensbedömningar avseende dataskydd samt både interna samråd (t.ex. ledningens godkännande av projektet eller interna beslut om konfidensintervall) och externa samråd (t.ex. med dataskyddsmyndigheten). Bilaga II innehåller ett antal exempel som belyser detta.

3.2.5.7 Artikel 47 Effektiv tillsyn

103. För att skydda de grundläggande rättigheterna och friheterna för de personer som påverkas av användningen av ansiktsigenkänningsteknik måste de behöriga dataskyddsmyndigheterna kunna utöva en effektiv tillsyn. Att varje dataskyddsmyndighet förfogar över de personella, tekniska och finansiella resurser samt de lokaler och den infrastruktur som behövs är en förutsättning för att de ska

kunna utföra sina uppgifter och utöva sina befogenheter effektivt[66]. Ännu viktigare än antalet tillgängliga medarbetare är de sakkunnigas kompetens, vilken bör täcka ett mycket brett spektrum av frågor – från brottsutredningar och polissamarbete till stordataanalys och AI. Medlemsstaterna bör därför säkerställa att tillsynsmyndigheternas resurser är lämpliga och tillräckliga för att de ska kunna fullgöra sitt uppdrag att skydda de registrerades rättigheter och noga följa all utveckling i detta avseende[67].

4 SLUTSATS

104. Användningen av ansiktsigenkänningsteknik medför behandling av stora mängder personuppgifter, däribland särskilda kategorier av uppgifter. Ansiktet och, mer allmänt, de biometriska uppgifterna är permanent och oåterkalleligt kopplade till en persons identitet. Användningen av ansiktsigenkänning har därför en direkt eller indirekt inverkan på flera av de grundläggande rättigheter och friheter som fastställs i Europeiska unionens stadga om de grundläggande rättigheterna. Denna inverkan kan gå utöver skyddet av privatliv och personuppgifter och även omfatta bland annat människans värdighet, rörelsefriheten och mötesfriheten. Detta är särskilt relevant på områdena brottsbekämpning och straffrätt.

105. EDPB inser att de brottsbekämpande myndigheterna måste ha tillgång till de bästa verktygen för att snabbt kunna identifiera gärningsmännen bakom terroristattentat och andra grova brott. Sådana verktyg bör emellertid användas i strikt överensstämmelse med den tillämpliga rättsliga ramen och endast om de uppfyller kraven på nödvändighet och proportionalitet enligt artikel 52.1 i stadgan. Även om modern teknik kan vara en del av lösningen är den inte på något sätt en patentlösning.

106. I vissa fall medför användningen av ansiktsigenkänningsteknik oacceptabelt höga risker för enskilda personer och samhället (s.k. röda linjer). Av dessa skäl har EDPB och EDPS uppmanat till ett allmänt förbud mot sådan användning[68].

107. Biometrisk fjärridentifiering av enskilda personer på allmänna platser medför en hög risk för intrång i enskildas privatliv och hör därmed inte hemma i ett demokratiskt samhälle, eftersom tekniken till sin natur är en form av massövervakning. Likaså anser EDPB att AI-stödda system för ansiktsigenkänning som kategoriserar enskilda personer på grundval av deras biometriska kännetecken i kluster efter etnicitet, kön, politiska åsikter eller sexuell läggning inte är förenliga med stadgan. EDPB är även övertygad om att användningen av ansiktsigenkänning eller liknande teknik för att dra slutsatser om fysiska personers känslor är ytterst olämplig och bör förbjudas, eventuellt med ett fåtal motiverade undantag. Dessutom anser EDPB att behandling av personuppgifter i ett brottsbekämpande sammanhang som skulle bygga på en databas som uppdateras genom massinsamling av personuppgifter på ett urskillningslöst sätt, t.ex. genom ”skrapning” av fotografier och ansiktsbilder som är tillgängliga online, särskilt via sociala nätverk, i sig inte skulle uppfylla det krav på absolut nödvändighet som föreskrivs i unionsrätten.

[66] Se kommissionens meddelande *Första rapporten om hur direktivet om uppgiftsskydd vid brottsbekämpning (EU) 2016/680 (dataskyddsdirektivet) tillämpas och fungerar*, COM(2022) 364 final, avsnitt 3.4.1.

[67] Se *Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62* (inte översatt till svenska), punkt 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

[68] Se det gemensamma yttrandet 5/2021 från EDPB och EDPS om förslaget till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

5 BILAGOR

Bilaga I: Stödmallar

Bilaga II: Praktisk vägledning för brottsbekämpande myndigheters förvaltning av ansiktsigenkänningsprojekt

Bilaga III: Praktiska exempel

BILAGA I – MALL FÖR BESKRIVNING AV SCENARIER

(Med informationsrutor för de aspekter som behandlas i scenariot)

Beskrivning av behandlingen:

- Beskrivning av behandlingen, sammanhang (samband med brott), ändamål

Uppgiftskälla:

- Typer av registrerade: ☐ Alla medborgare ☐ Dömda brottslingar ☐ Misstänkta personer
  ☐ Barn ☐ Andra sårbara registrerade
- Bildkälla: ☐ Allmänt tillgängliga platser ☐ Internet
  ☐ Privat aktör ☐ Andra fysiska personer ☐ Annan: .....

- Koppling till brott: ☐ Direkt tidsmässig ☐ Inte direkt tidsmässig
  ☐ Direkt geografisk ☐ Inte direkt geografisk
  ☐ Ej nödvändig

- Metod för inhämtning av uppgifter: ☐ På distans ☐ I ett bås eller i en kontrollerad miljö
- Sammanhang – påverkar andra grundläggande rättigheter:
  ☐ Nej
  Ja, närmare bestämt ☐ mötesfriheten
  ☐ yttrandefriheten
  ☐ övriga:.....
- Möjliga andra källor till information om den registrerade:
  ☐ Id-handling ☐ Användning av telefonautomat ☐ Registreringsskylt på fordon
  ☐ Övriga: .....

Referensdatabas (mot vilken inhämtade uppgifter jämförs):

- Typ: ☐ Databaser för allmänna ändamål ☐ Särskilda databaser med anknytning till brottsområdet
- Beskrivning av hur dessa referensdatabaser uppdaterats (och rättslig grund)
- Ändring av databasens ändamål (t.ex. att skydd av privat egendom var det primära målet):
  ☐ JA
  ☐ NEJ

Algoritm:

- Typ av behandling:☐ En mot en-verifiering (autentisering)☐ En mot många-identifiering
- Överväganden om noggrannhet
- Tekniska skyddsåtgärder

Resultat:

- Inverkan: ☐ Direkt (t.ex. den registrerade kan komma att gripas eller förhöras, kan bli utsatt för diskriminerande beteende)

  ☐ Inte direkt (Används för statistiska modeller, inga allvarliga rättsliga åtgärder mot registrerade)

- Automatiserat beslut: ☐ JA ☐ NEJ
- Lagringstid

Rättslig analys:

- Analys av nödvändighet och proportionalitet – ändamål/brottets allvarlighet/antal personer som inte är inblandade men som påverkas av behandlingen
- Typ av förhandsinformation till den registrerade: ☐ Vid inträde till det specifika området

  ☐ På den brottsbekämpande myndighetens allmänna webbplats

  ☐ På den brottsbekämpande myndighetens webbplats för den specifika behandlingen

  ☐ Annan: .....
- Tillämplig rättslig ram:

  ☐ Brottsdatadirektivet till största delen kopierad till nationell lagstiftning

  ☐ Allmän nationell lagstiftning för brottsbekämpande myndigheters användning av biometriska uppgifter

  ☐ Särskild nationell lagstiftning för denna behandling (ansiktsigenkänning) för den behöriga myndigheten

  ☐ Särskild nationell lagstiftning för denna behandling (automatiserat beslut)

Slutsats:

Allmänna överväganden om huruvida den beskrivna behandlingen sannolikt är förenlig med unionsrätten (och hänvisning till rättsliga villkor)

BILAGA II – PRAKTISK VÄGLEDNING FÖR BROTTSBEKÄMPANDE MYNDIGHETERS FÖRVALTNING AV ANSIKTSIGENKÄNNINGSPROJEKT

I denna bilaga ges ytterligare praktisk vägledning för brottsbekämpande myndigheter som planerar att inleda projekt som inbegriper teknik för ansiktsigenkänning. Bilagan innehåller information om organisatoriska och tekniska åtgärder som bör övervägas under genomförandet av sådana projekt, men det finns inte någon uttömmande förteckning över vilka steg eller åtgärder som bör vidtas. Den bör även läsas tillsammans med EDPB:s riktlinjer 3/2019 om behandling av personuppgifter genom videoenheter[69] samt EU-/EES-förordningar och EDPB:s riktlinjer om användning av artificiell intelligens.

Denna bilaga innehåller riktlinjer som bygger på antagandet att brottsbekämpande myndigheter kommer att upphandla ansiktsigenkänningsteknik (som en färdig produkt). Om de brottsbekämpande myndigheterna planerar att utveckla (träna) ansiktsigenkänningstekniken tillkommer ytterligare krav på de dataset som ska användas för träning, validering och provning under utvecklingen samt rollerna/åtgärderna för utvecklingsmiljön. På liknande sätt kan en färdig produkt kräva ytterligare justeringar för den avsedda användningen, varvid de ovannämnda kraven för valet av dataset för träning, validering och provning bör vara uppfyllda.

Att tillhöra samma brottsbekämpande myndighet ger inte i sig fullständig tillgång till alla biometriska uppgifter. Precis som för alla andra kategorier av personuppgifter får biometriska uppgifter som samlas in för ett visst brottsbekämpande ändamål enligt en specifik rättslig grund inte användas utan en lämplig rättslig grund för något annat brottsbekämpande ändamål (artikel 4.2 i direktiv (EU) 2016/680 [*brottsdatadirektivet*]). Utveckling eller träning av ett verktyg för ansiktsigenkänning anses dessutom vara ett annat ändamål, och det bör bedömas om behandlingen av biometriska uppgifter för att mäta prestanda/träna tekniken så att de registrerade inte påverkas av låg prestanda är nödvändig och proportionell med beaktande av det ursprungliga ändamålet.

1. ROLLER OCH ANSVARSOMRÅDEN

Om en brottsbekämpande myndighet inför ansiktsigenkänningsteknik för att fullgöra uppgifter som omfattas av brottsdatadirektivet (förebygga, förhindra, utreda, avslöja eller lagföra brott etc., enligt artikel 3 i brottsdatadirektivet) kan myndigheten betraktas som personuppgiftsansvarig för tekniken. Brottsbekämpande myndigheter består emellertid av flera enheter/avdelningar som kan vara delaktiga i denna behandling, antingen genom att fastställa processen för tillämpning av ansiktsigenkänningsteknik eller genom att tillämpa tekniken i praktiken. På grund av teknikens särskilda egenskaper kan olika enheter behöva vara delaktiga för att antingen stödja mätningarna av teknikens prestanda eller för att träna den ytterligare.

I ett projekt som inbegriper ansiktsigenkänningsteknik kan flera berörda parter[70] inom de brottsbekämpande myndigheterna behöva delta, nämligen följande:

---

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

[70] De roller som beskrivs är vägledande för de olika berörda parterna och deras ansvarsområden i ett projekt med ansiktsigenkänningsteknik. Även om det språk som används för att beskriva rollerna i denna bilaga har en allmän karaktär måste varje brottsbekämpande myndighet definiera och tilldela liknande roller i sin organisation. En enhet kan ha fler än en roll, till exempel processansvarig och förvaltare av referensdatabasen eller processansvarig och ansvarig för avdelningen för informationsteknik, AI och/eller datavetenskap (om enheten har all nödvändig teknisk kunskap).

- Högsta ledningen – godkänner projektet efter att ha vägt riskerna mot de potentiella fördelarna.
- Dataskyddsombudet och/eller den brottsbekämpande myndighetens juridiska avdelning – hjälper till att bedöma om genomförandet av ett visst projekt för ansiktsigenkänningsteknik är lagligt, bistår i genomförandet av konsekvensbedömningen avseende dataskydd, säkerställer respekten för och utövandet av de registrerades rättigheter.
- Processansvarig – agerar som den specifika enhet inom den behöriga brottsbekämpande myndigheten som ska utveckla projektet för ansiktsigenkänning, besluta om detaljerna i projektet, inbegripet systemets prestandakrav, besluta om ett lämpligt rättvisemått, fastställa konfidensgraden[71], fastställa acceptabla tröskelvärden för snedvridning, identifiera de potentiella risker som projektet innebär för enskilda personers rättigheter och friheter (genom samråd med dataskyddsombudet och avdelningen för informationsteknik, AI och/eller datavetenskap – se nedan) samt presentera dem för den högsta ledningen. Den processansvarige ska även samråda med förvaltaren av referensdatabasen innan beslut fattas om detaljerna i projektet, för att klargöra såväl referensdatabasens användningsområde som dess tekniska detaljer. Om en upphandlad ansiktsigenkänningsteknik ska tränas ytterligare kommer den processansvarige även att ansvara för valet av dataset. Eftersom den processansvarige ansvarar för att utveckla och besluta om detaljerna i projektet ingår även genomförandet av konsekvensbedömningen avseende dataskydd i den processansvariges ansvarsområde.
- Avdelningen för informationsteknik, AI och/eller datavetenskap – bistår vid genomförandet av en konsekvensbedömning avseende dataskydd, förklarar de parametrar som finns tillgängliga för att mäta systemets prestanda, rättvisa[72] och möjliga snedvridning, genomför tekniken och de tekniska skyddsåtgärderna, förhindrar obehörig åtkomst till insamlade uppgifter, cyberattacker osv. Vid omträning av ett upphandlat system för ansiktsigenkänning tränar avdelningen systemet på grundval av det dataset som tillhandahållits av den processansvarige. Denna avdelning har även ansvar för att införa åtgärder som minskar de risker som de processansvariga gemensamt har identifierat (t.ex. attacker genom modellinferens och andra AI-specifika risker).
- Slutanvändare (t.ex. poliser i yttre tjänst eller i kriminaltekniska laboratorier) – utför en jämförelse mot databasen, granskar kritiskt resultaten med beaktande av tidigare bevis och ger feedback till den processansvarige om falska positiva resultat och indikationer på möjlig diskriminering.
- Förvaltare av referensdatabasen – den specifika enhet inom den behöriga brottsbekämpande myndigheten som ansvarar för att sammanställa och förvalta referensdatabasen, dvs. den databas mot vilken bilder kommer att jämföras, däribland genom att radera ansiktsbilderna efter den fastställda lagringsperioden. Denna databas kan skapas specifikt för det planerade ansiktsigenkänningsprojektet eller redan finnas tillgänglig för kompatibla ändamål. Referensdatabasens förvaltare ansvarar för att fastställa när och under vilka omständigheter ansiktsbilder får lagras och för att fastställa de relaterade lagringskraven (baserat på tid eller andra kriterier).

Eftersom införandet och användningen av ansiktsigenkänningsteknik i de flesta fall medför en hög risk för de registrerades rättigheter och friheter bör tillsynsmyndigheten för dataskydd också delta i det förhandssamråd som krävs enligt artikel 28 i brottsdatadirektivet.

[71] Konfidensgraden är konfidensnivån för förutsägelsen (matchningen), uttryckt som en sannolikhet. T.ex. vid en jämförelse mellan två mallar är sannolikheten 90 % för att dessa tillhör samma person. Konfidensgraden är inte samma som ansiktsigenkänningsteknikens prestanda, men den påverkar prestandan: ju högre konfidensgrad, desto färre falska positiva och desto fler falska negativa resultat av ansiktsigenkänningen.

[72] Rättvisa kan definieras som avsaknaden av orättvis och olaglig diskriminering, till exempel på grund av kön eller ras.

2. FÖRE UPPHANDLINGEN AV ANSIKTSIGENKÄNNINGSSYSTEMET

Den processansvarige vid en brottsbekämpande myndighet bör först och främst ha en god inblick i den eller de processer som ligger till grund för användningen av ansiktsigenkänningsteknik (användningsfallet) och se till att det finns en rättslig grund för den planerade användningen. För detta ändamål måste den processansvarige göra följande:

- Beskriva användningsfallet formellt. Beskrivningen ska omfatta det problem som ska lösas och hur ansiktsigenkänningstekniken bidrar till lösningen. Det ska även finnas en översikt över den process (uppgift) inom vilken tekniken kommer att tillämpas. I detta avseende bör de brottsbekämpande myndigheterna åtminstone dokumentera följande[73]:
  - Vilka kategorier av personuppgifter som registreras under processen.
  - Vilka mål och konkreta ändamål tekniken kommer att användas till, inbegripet de möjliga konsekvenserna för den registrerade efter en matchning.
  - När och hur ansiktsbilderna kommer att samlas in (inbegripet information om sammanhanget för insamlingen, t.ex. vid gaten på en flygplats, videofilmer från säkerhetskameror utanför en butik där ett brott har begåtts osv., samt vilka kategorier av registrerade vilkas biometriska uppgifter kommer att behandlas).
  - Vilken databas bilderna ska jämföras mot (referensdatabasen) samt information om hur databasen skapades, dess storlek och kvaliteten på de biometriska uppgifter som finns lagrade i den.
  - Vilka personer hos de brottsbekämpande myndigheterna som kommer att vara behöriga att använda systemet för ansiktsigenkänning och tillämpa det i samband med brottsbekämpning (deras profiler och åtkomsträttigheter måste fastställas av den processansvarige).
  - Den planerade lagringsperioden för de inmatade uppgifterna, eller den tidpunkt som kommer att utgöra slutet på denna period (till exempel när det straffrättsliga förfarande för vilket uppgifterna ursprungligen samlades in avslutas i enlighet med nationell processrätt), samt eventuella efterföljande åtgärder (radering av uppgifterna, anonymisering, användning för statistiska ändamål eller forskningsändamål osv.).
  - Genomförandet av loggning och tillgången till loggar och register.
  - Prestandamåtten (t.ex. noggrannhet, precision, träffmängd och F1-värde) samt deras lägsta godtagbara tröskelvärden[74].
  - En uppskattning av hur många personer som kommer att granskas med ansiktsigenkänningstekniken samt under vilken tidsperiod/vid vilket tillfälle.
- Utföra en bedömning av nödvändighet och proportionalitet[75]. Det faktum att tekniken finns tillgänglig bör inte vara drivkraften för att tillämpa den. Den processansvarige måste först bedöma om det finns en lämplig rättslig grund för den planerade behandlingen. För detta ändamål måste dataskyddsombudet och rättstjänsten rådfrågas. Drivkraften för att införa

[73] Bilaga I innehåller en förteckning över faktorer som hjälper den personuppgiftsansvarige att beskriva ett användningsfall för ansiktsigenkänningsteknik.

[74] Det finns olika mått för att utvärdera prestandan hos ett system för ansiktsigenkänning. Varje mått ger olika uppfattningar om systemets resultat, och deras användbarhet när det gäller att ge en heltäckande bild av systemets prestanda beror på användningsfallet. Om fokus ligger på att uppnå en hög andel korrekta matchningar av ett ansikte kan mått som precision och träffmängd användas. Dessa mått visar emellertid inte hur väl ansiktsigenkänningstekniken hanterar negativa exempel (hur många som matchades felaktigt av systemet). Den processansvarige bör, med stöd av avdelningen för informationsteknik, AI och datavetenskap, kunna fastställa prestandakraven och uttrycka dem med det lämpligaste måttet beroende på användningsfallet.

[75] Ytterligare åtgärder kan övervägas för att ta hänsyn till nödvändigheten när det gäller systemets anpassning och användning, vilket innebär att beskrivningen av användningsfallet kan ändras något under bedömningen av nödvändighet och proportionalitet.

ansiktsigenkänningsteknik bör vara att den är en nödvändig och proportionerlig lösning på ett specifikt problem som fastställts av de brottsbekämpande myndigheterna. Detta måste bedömas utifrån ändamålet/brottets allvarlighet/antalet personer som inte är inblandade men som påverkas av ansiktsigenkänningssystemet. Vid bedömningen av om behandlingen är laglig bör hänsyn åtminstone tas till brottsdatadirektivet[76], den allmänna dataskyddsförordningen[77] [78], befintliga rättsliga ramar för AI[79] och de riktlinjer som tillhandahålls av tillsynsmyndigheterna för dataskydd (t.ex. EDPB:s riktlinjer 3/2019 för behandling av personuppgifter genom videoenheter[80]). Dessa EU-rättsakter bör alltid jämföras med de tillämpliga nationella kraven, särskilt på straffprocessrättens område. Proportionalitetsbedömningen bör omfatta vilka av de registrerades grundläggande rättigheter som kan komma att påverkas (utöver privatliv och dataskydd). Den bör även beskriva och ta hänsyn till eventuella begränsningar (eller avsaknad av begränsningar) i ansiktsigenkänningssystemet för varje användningsfall, till exempel om systemet kommer att användas fortlöpande eller tillfälligt och om det kommer att begränsas till ett geografiskt område.

- Utföra en konsekvensbedömning avseende dataskydd[81]. En konsekvensbedömning avseende dataskydd bör genomföras eftersom införandet av ansiktsigenkänningsteknik på brottsbekämpningsområdet riskerar att leda till en hög risk för enskilda personers rättigheter och friheter[82]. Konsekvensbedömningen bör särskilt innehålla en allmän beskrivning av den planerade behandlingen[83], en bedömning av riskerna för de registrerades rättigheter och friheter[84], de åtgärder som planeras för att hantera dessa risker, skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att påvisa efterlevnad. Eftersom

[76] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

[77] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

[78] Om personuppgifter måste behandlas i samband med ett vetenskapligt projekt som syftar till att undersöka användningen av ansiktsigenkänningsteknik, och om den behandlingen inte omfattas av artikel 4.3 i brottsdatadirektivet, är den allmänna dataskyddsförordningen i allmänhet tillämplig (artikel 9.2 i brottsdatadirektivet). När det gäller pilotprojekt som följs av brottsbekämpande insatser är det brottsdatadirektivet som tillämpas.

[79] Det finns till exempel ett förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter, men det har ännu inte införts som en förordning.

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

[81] Ytterligare vägledning om konsekvensbedömningar avseende dataskydd finns i följande dokument: *Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679*, WP 248 rev. 01, finns på https://ec.europa.eu/newsroom/article29/items/611236 och EDPS:s verktygslåda *Accountability on the ground* (inte översatt till svenska), del II, finns på https://edps.europa.eu/node/4582_en.

[82] Ansiktsigenkänningsteknik kan, beroende på användningsfallet, omfattas av följande kriterier som medför högriskbehandling (enligt riktlinjerna om konsekvensbedömning avseende dataskydd, WP 248 rev. 01): systematisk övervakning, uppgifter som behandlas i stor omfattning, matchande eller kombinerande uppgiftsserier, innovativ användning eller tillämpning av nya tekniska eller organisatoriska lösningar.

[83] Beskrivningen av behandlingen och nödvändighets- och proportionalitetsbedömningen, såsom beskrivits i ovanstående steg, ingår också i konsekvensbedömningen avseende dataskydd, med undantag av riskbedömningen. Vid behov ska en mer detaljerad beskrivning av flödena av personuppgifter tillhandahållas i konsekvensbedömningen avseende dataskydd.

[84] Analysen av riskerna för de registrerade bör omfatta risker avseende platsen där ansiktsbilderna ska jämföras (lokalt/på distans), risker avseende personuppgiftsbiträden/underentreprenörer samt risker som är specifika för maskininlärning om denna teknik tillämpas (t.ex. dataförgiftning och antagonistiska exempel).

konsekvensbedömningen avseende dataskydd är en pågående process bör nya delar av behandlingen läggas till och riskbedömningen uppdateras i varje skede av projektet.

- Inhämta godkännande från högsta ledningen genom att förklara riskerna för de registrerades rättigheter och friheter (utifrån användningsfallet och tekniken) och de respektive riskhanteringsplanerna.

3. UNDER UPPHANDLINGEN OCH FÖRE INFÖRANDET AV ANSIKTSIGENKÄNNINGSTEKNIKEN

- Fastställa kriterierna för valet av ansiktsigenkänningsteknik (algoritm). Den processansvarige bör fastställa kriterierna för valet av algoritm, med stöd av avdelningen för informationsteknik, AI och/eller datavetenskap. I praktiken skulle dessa kriterier omfatta de mätvärden för rättvisa och prestanda som fastställts i beskrivningen av användningsfallet. Kriterierna bör även inbegripa information om vilka uppgifter som har använts för att träna algoritmen. För att minska snedvridningen måste det dataset som används för träning, provning och validering omfatta ett tillräckligt urval av egenskaper (t.ex. ålder, kön och ras) hos de registrerade som ska omfattas av ansiktsigenkänningstekniken. Leverantören av ansiktsigenkänningstekniken bör tillhandahålla information om och mått för de dataset som använts för träning, provning och validering av tekniken och beskriva vilka åtgärder som vidtagits för att mäta och minska eventuell olaglig diskriminering och snedvridning. Om det är möjligt måste den processansvarige kontrollera om leverantören hade en rättslig grund för att använda detta dataset i syfte att träna algoritmerna (baserat på den information som leverantören ska göra tillgänglig). Den processansvarige bör även säkerställa att leverantören av ansiktsigenkänningstekniken tillämpar säkerhetsstandarder för biometriska uppgifter, däribland ISO/IEC 24745, som ger vägledning för skyddet av biometriska uppgifter enligt olika krav på konfidentialitet, integritet och förnyelse/återkallelse under lagringen och överföringen samt krav och riktlinjer för en säker och konfidentiell hantering och behandling av biometriska uppgifter.

- Träna om algoritmen (om det är nödvändigt). Den processansvarige bör säkerställa att de upphandlade tjänsterna även inbegriper en finjustering av ansiktsigenkänningssystemet för att uppnå högre noggrannhet innan det används. Om det upphandlade ansiktsigenkänningssystemet behöver tränas ytterligare för att uppfylla noggrannhetskraven måste den processansvarige, förutom att fatta beslutet om omträning, besluta, med stöd av avdelningen för informationsteknik, AI och/eller datavetenskap, vilket lämpligt och representativt dataset som ska användas och kontrollera att denna användning av uppgifterna är laglig.
- Fastställa lämpliga skyddsåtgärder för att hantera risker med anknytning till säkerhet, snedvridning och låg prestanda. Detta inbegriper inrättandet av en process för att övervaka ansiktsigenkänningstekniken när den har tagits i bruk (loggning och återkoppling för att resultaten ska vara korrekta och rättvisa). Dessutom måste det säkerställas att de risker som är specifika för vissa maskininlärnings- och ansiktsigenkänningssystem (t.ex. dataförgiftning, antagonistiska exempel, modellinversion och whitebox-inferens) identifieras, mäts och begränsas. Den processansvarige bör även fastställa lämpliga skyddsåtgärder för att säkerställa att lagringskraven för de biometriska uppgifter som ingår i datasetet för omträning respekteras.
- Dokumentera systemet för ansiktsigenkänning. Dokumentationen bör omfatta en allmän beskrivning av ansiktsigenkänningssystemet, en detaljerad beskrivning av systemets beståndsdelar och processen för dess inrättande, detaljerad information om systemets övervakning, funktion och kontroll samt en ingående beskrivning av de riskbegränsande åtgärderna. I dokumentationen ska de viktigaste delarna av systemets beskrivning från tidigare

faser ingå (se ovan). Dessa kommer emellertid att utökas med information som rör övervakning av prestanda och tillämpning av ändringar i systemet, inbegripet eventuella versionsuppdateringar och/eller omträningar.

- Utarbeta användarhandböcker som förklarar tekniken och användningsområdena. Dessa måste innefatta en tydlig förklaring av alla scenarier och förutsättningar under vilka ansiktsigenkänningstekniken kommer att användas.
- Utbilda slutanvändarna i hur tekniken ska användas. Denna utbildning måste omfatta teknikens kapacitet och begränsningar, så att användarna kan förstå under vilka omständigheter det är nödvändigt att tillämpa den och i vilka fall den kan vara missvisande. Utbildningen kommer även att bidra till att minska riskerna med att inte kontrollera/kritisera algoritmens resultat.
- Samråda med tillsynsmyndigheten för dataskydd, i enlighet med artikel 28.1 b i brottsdatadirektivet. Tillhandahålla information enligt artikel 13 i brottsdatadirektivet för att informera de registrerade om behandlingen och deras rättigheter. Denna information måste vara riktad till de registrerade på ett lämpligt språk, så att de kan förstå behandlingen och få inblick i de grundläggande delarna av tekniken, däribland noggrannhetsgrader, träningsdataset och åtgärder som vidtagits för att undvika att algoritmen är diskriminerande eller inte tillräckligt noggrann.

4. REKOMMENDATIONER EFTER INFÖRANDET AV ANSIKTSIGENKÄNNINGSTEKNIK

- Säkerställ mänskligt ingripande och övervakning av resultaten. Vidta aldrig någon åtgärd som rör en enskild person enbart på grundval av resultatet av ansiktsigenkänningsteknik (detta skulle innebära en överträdelse av artikel 11 i brottsdatadirektivet – automatiserat individuellt beslutsfattande med rättsliga eller andra liknande följder för den registrerade). Se till att en tjänsteman hos den brottsbekämpande myndigheten granskar resultaten av ansiktsigenkänningstekniken. Se också till att brottsbekämpande myndigheter undviker automationssnedvridning genom att undersöka motstridig information och kritiskt ifrågasätta teknikens resultat. För att uppnå detta är det viktigt med kontinuerlig utbildning och information till slutanvändarna. Samtidigt bör den högsta ledningen se till att det finns tillräckliga personalresurser för en effektiv tillsyn. Personalen måste få tillräckligt med tid för att kritiskt ifrågasätta teknikens resultat. Registrera, mät och bedöm i vilken utsträckning den mänskliga tillsynen ändrar det ursprungliga beslut som fattats med hjälp av ansiktsigenkänningstekniken.
- Övervaka och hantera förändringar i modellen för ansiktsigenkänning (prestandaförsämring) när den är i produktion.
- Inrätta ett förfarande för att omvärdera riskerna och säkerhetsåtgärderna regelbundet och åtminstone varje gång tekniken eller användningsfallet förändras.
- Dokumentera eventuella ändringar av systemet under hela dess livscykel (t.ex. uppgraderingar och omträning).
- Inrätta ett förfarande och nödvändig teknisk kapacitet för att hantera begäranden om åtkomst från de registrerade. Om det finns ett behov av att tillhandahålla uppgifter till de registrerade måste det finnas teknisk kapacitet för att hämta dem innan en begäran görs.
- Se till att rutiner har införts för att motverka dataintrång. Om en personuppgiftsincident som inbegriper biometriska uppgifter skulle inträffa kommer riskerna sannolikt att vara höga. Alla berörda användare bör vara medvetna om de relevanta förfaranden som ska följas, och dataskyddsombudet och de registrerade bör informeras omgående.

BILAGA III – PRAKTISKA EXEMPEL

Ansiktsigenkänning kan användas för en rad olika ändamål, t.ex. vid gränsövergångar och i andra kontrollerade miljöer, i samband med dubbelkontroll mot uppgifter i polisdatabaser eller personuppgifter som den registrerade har offentliggjort på ett tydligt sätt samt i direktsända kameraflöden (ansiktsigenkänning i realtid). Detta gör att riskerna när det gäller skyddet av personuppgifter och andra grundläggande rättigheter och friheter varierar avsevärt i de olika användningsfallen. För att underlätta den bedömning av nödvändighet och proportionalitet som bör föregå ett beslut om införande av ansiktsigenkänningsteknik innehåller dessa riktlinjer en icke uttömmande förteckning över möjliga tillämpningar på brottsbekämpningsområdet.

De scenarier som presenteras och bedöms bygger på **hypotetiska** situationer och är avsedda att illustrera viss konkret användning av ansiktsigenkänningsteknik. De kan ge stöd till överväganden från fall till fall eller användas för att fastställa en övergripande ram. Förteckningen över scenarier är inte uttömmande och påverkar inte pågående eller framtida förfaranden som inletts av en nationell tillsynsmyndighet när det gäller utformningen, provningen eller genomförandet av ansiktsigenkänningsteknik. Scenarierna syftar endast till att illustrera den vägledning som redan ges till beslutsfattare, lagstiftare och brottsbekämpande myndigheter i detta dokument för att säkerställa full överensstämmelse med EU:s regelverk för personuppgiftsskydd när de utformar och planerar införandet av teknik för ansiktsigenkänning. Det är viktigt att komma ihåg att förekomsten eller avsaknaden av vissa faktorer kan leda till ett annat resultat av nödvändighets- och proportionalitetsbedömningen även i liknande situationer där ansiktsigenkänningsteknik används.

1 SCENARIO 1

1.1. Beskrivning

Ett system för automatiserad gränskontroll som möjliggör automatiserad gränspassage för EU-medborgare och andra resenärer genom att autentisera den biometriska bild som finns lagrad i resenärens elektroniska resehandling och verifiera att passageraren är handlingens rättmätiga innehavare.

Denna verifiering/autentisering omfattar endast ”en mot en”-ansiktsigenkänning och utförs i en kontrollerad miljö (t.ex. vid elektroniska spärrar på flygplatser). De biometriska uppgifterna registreras när resenären uttryckligen uppmanas att titta in i kameran vid den elektroniska spärren och jämförs sedan med uppgifterna i den uppvisade handlingen (t.ex. ett pass eller id-kort), vilken ska ha utfärdats i enlighet med särskilda tekniska krav.

Även om behandlingen i sådana fall i princip faller utanför tillämpningsområdet för brottsdatadirektivet kan resultatet av verifieringen även användas i samband med matchning av (alfanumeriska) uppgifter om personen i databaser för brottsbekämpning som en del av gränskontrollen. Den kan därmed ha betydande rättslig verkan för den registrerade, t.ex. ett gripande om det finns en registrering i Schengens informationssystem. Under särskilda omständigheter kan de biometriska uppgifterna även användas för att söka efter matchningar i databaser för brottsbekämpning (i ett sådant fall skulle ”en mot många”-identifiering utföras i detta steg).

Resultatet av behandlingen av den biometriska bilden har en direkt inverkan på den registrerade, eftersom han eller hon inte får passera gränspassagen förrän verifieringen är godkänd. Om den registrerade inte kan identifieras måste gränsvakterna göra en andra kontroll för att säkerställa att den registrerade är en annan person än personen på bilden i id-handlingen.

Om en registrering konstateras i Schengens informationssystem eller en nationell databas måste gränsvakterna utföra en andra verifiering och därefter vidta nödvändiga åtgärder, t.ex. gripa personen eller informera de berörda myndigheterna.

Uppgiftskälla:

- Typer av registrerade: ☒ Alla personer som passerar gränserna
- Bildkälla: ☒ Annan (id-handling)
- Koppling till brott: ☒ Ej nödvändig
- Metod för inhämtning av uppgifter: ☒ I ett bås eller i en kontrollerad miljö
- Sammanhang – påverkar andra grundläggande rättigheter: Ja, närmare bestämt ☒ rätten till fri rörlighet ☒ rätten till asyl

Referensdatabas (mot vilken inhämtade uppgifter jämförs):

- Typ: ☒ Särskilda databaser med anknytning till gränskontroll

Algoritm:

- Typ av behandling: ☒ ”En mot en”-verifiering (autentisering)

Resultat:

- Inverkan ☒ Direkt (den registrerade tillåts eller nekas inresa)
- Automatiserat beslut: ☒ Ja

1.2. Tillämplig rättslig ram

Sedan 2004 måste pass och andra resehandlingar som utfärdas av medlemsstaterna innehålla en biometrisk ansiktsbild som lagras i ett elektroniskt chip i handlingen, i enlighet med rådets förordning (EG) nr 2252/2004[85].

I kodexen om Schengengränserna[86] fastställs kraven för gränskontroller av personer vid de yttre gränserna. För EU-medborgare och andra personer som åtnjuter fri rörlighet enligt unionsrätten bör kontrollerna åtminstone bestå av en verifiering av resehandlingarna, vid behov med hjälp av tekniska utrustning. Kodexen om Schengengränserna har senare ändrats genom förordning (EU) 2017/2225[87], som bland annat omfattar definitioner av *elektroniska spärrar*, *system för automatiserad gränskontroll* och *självbetjäningssystem* samt möjligheten att behandla biometriska uppgifter för utförande av inresekontroller.

Det kan därför antas att det finns en tydlig och förutsägbar rättslig grund som tillåter denna form av personuppgiftsbehandling. Dessutom antas den rättsliga ramen på unionsnivå, varefter den är direkt tillämplig för medlemsstaterna.

1.3. Nödvändighet och proportionalitet – ändamål/brottets allvarlighet

Verifiering av EU-medborgares identitet med hjälp av biometriska bilder vid en automatiserad gränskontroll är en del av kontrollerna vid EU:s yttre gränser. Följaktligen har verifieringen en direkt koppling till gränssäkerheten, vilket är ett mål av allmänt samhällsintresse som erkänns av unionen. Systemet för automatiserad gränskontroll bidrar även till att påskynda behandlingen av passagerare och minska risken för mänskliga misstag. Dessutom är ingreppets räckvidd, omfattning och intensitet i detta scenario mycket mer begränsad jämfört med andra former av ansiktsigenkänning.

[85] Rådets förordning (EG) nr 2252/2004 av den 13 december 2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna.

[86] Europaparlamentets och rådets förordning (EU) 2016/399 av den 9 mars 2016 om en unionskodex om gränspassage för personer (kodex om Schengengränserna).

[87] Europaparlamentets och rådets förordning (EU) 2017/2225 av den 30 november 2017 om ändring av förordning (EU) 2016/399 vad gäller användningen av in- och utresesystemet.

Behandlingen av biometriska uppgifter leder emellertid till ytterligare risker för de registrerade som måste hanteras och minskas på lämpligt sätt av den behöriga myndighet som inför och använder ansiktsigenkänningstekniken.

1.4. Slutsats

Verifieringen av EU-medborgares identitet i samband med automatiserad gränskontroll är en nödvändig och proportionell åtgärd så länge som lämpliga skyddsåtgärder har vidtagits, särskilt tillämpningen av principerna om ändamålsbegränsning, uppgiftskvalitet, öppenhet och en hög säkerhetsnivå.

2 SCENARIO 2

2.1. Beskrivning

De brottsbekämpande myndigheterna inrättar ett system för identifiering av barn som förts bort mot sin vilja. En behörig polis får under stränga villkor jämföra biometriska uppgifter om ett barn som misstänks ha förts bort mot en databas över bortförda barn, med det enda syftet att identifiera minderåriga som kan stämma in på beskrivningen av det försvunna barn för vilket en utredning har inletts och en anmälan har utfärdats.

Behandlingen skulle innebära att en persons ansikte eller ansiktsbild, som motsvarar beskrivningen av ett försvunnet barn, jämförs med bilderna i databasen. Denna behandling skulle ske i specifika fall och inte systematiskt.

Den databas som jämförelsen kommer att göras mot innehåller bilder på försvunna barn som misstänks ha förts bort eller utsatts för fara för sitt liv eller sin fysiska hälsa och för vilka en brottsutredning har inletts av en rättslig myndighet och en anmälan om bortförande av barn har utfärdats. Uppgifterna samlas in inom ramen för förfaranden som fastställts av den behöriga brottsbekämpande myndigheten, dvs. av poliser som är bemyndigade att utföra rättsliga polisuppdrag. Följande kategorier av personuppgifter registreras:

- Identitet, smeknamn, alias, släktskap, nationalitet, adresser, e-postadresser och telefonnummer.
- Födelsedatum och födelseort.
- Information om föräldraskap.
- Fotografi med tekniska egenskaper som möjliggör användning av ansiktsigenkänning och andra fotografier.

Resultaten av jämförelsen måste även granskas och verifieras av en behörig tjänsteman för att bekräfta tidigare bevis gentemot resultaten av jämförelsen och utesluta eventuella falska positiva resultat.

Bilder på barn och barnens personuppgifter får endast lagras under den tid som registreringen gäller och måste raderas omedelbart efter att det straffrättsliga förfarandet har avslutats i enlighet med de nationella förfaranden för vilka de har förts in i databasen.

Även om lagringsperioden för biometriska uppgifter i databasen kan vara relativt lång och fastställd enligt nationell lagstiftning utgör de registrerades utövande av sina rättigheter, särskilt rätten till rättelse och radering, en ytterligare garanti för att begränsa ingreppet i de berörda registrerades rätt till personuppgiftsskydd.

Uppgiftskälla:

- Typer av registrerade: ☒ Barn
- Bildkälla ☒ Annan: inte fastställd i förväg, barn som misstänks ha förts bort
- Koppling till brott: ☒ Inte direkt tidsmässig ☒ Inte direkt geografisk
- Metod för inhämtning av uppgifter: ☒ I ett bås eller i en kontrollerad miljö
- Sammanhang – påverkar andra grundläggande rättigheter: ☒ Ja, närmare bestämt ☒ övriga

Referensdatabas (mot vilken inhämtade uppgifter jämförs):

- Typ: ☒ Särskild databas

Algoritm:

- Typ av behandling: ☒ En mot många-identifiering

Resultat:

- Inverkan: ☒ Direkt
- Automatiserat beslut: ☒ NEJ, obligatorisk granskning utförd av en behörig tjänsteman

Rättslig analys:

- Tillämplig rättslig ram: ☒ Särskild nationell lagstiftning för denna behandling (ansiktsigenkänning)

2.2. Tillämplig rättslig ram

I nationell lagstiftning föreskrivs en särskild rättslig ram för inrättandet av databasen, däribland ändamålen med behandlingen samt kriterierna för hur databasen ska fyllas med uppgifter, göras tillgänglig och användas. De lagstiftningsåtgärder som krävs för dess genomförande omfattar även fastställandet av en lagringsperiod samt hänvisningar till de tillämpliga principerna om integritet och konfidentialitet. I lagstiftningsåtgärderna föreskrivs även formerna för tillhandahållandet av information till den registrerade, i detta fall personen eller personerna med föräldraansvar, samt utövandet av den registrerades rättigheter och i tillämpliga fall eventuella begränsningar. När förslaget till respektive lagstiftningsåtgärd utarbetas måste den nationella tillsynsmyndigheten rådfrågas.

2.3. Nödvändighet och proportionalitet – ändamål/brottets allvarlighet/antal personer som inte är inblandade men som påverkas av behandlingen

Villkor och skyddsåtgärder för behandlingen

En jämförelse med hjälp av ansiktsigenkänning får endast utföras av en behörig tjänsteman som en sista utväg om det inte finns några andra mindre inkräktande metoder och om jämförelsen är absolut nödvändig, till exempel om äktheten hos en resande minderårigs identitetshandling kan betvivlas och/eller om en granskning av tidigare bevis och insamlat material tyder på en möjlig överensstämmelse med beskrivningen av ett försvunnet barn som omfattas av en brottsutredning.

En ytterligare säkerhetsåtgärd är att den behöriga tjänstemannen är skyldig att granska och verifiera ansiktsigenkänningen för att bekräfta tidigare bevis gentemot resultatet av jämförelsen och utesluta eventuella falska positiva resultat.

Eftersträvade mål

Inrättandet av databasen främjar ett antal viktiga mål av allmänt samhällsintresse, särskilt att förebygga, förhindra, utreda, avslöja eller lagföra brott, verkställa straffrättsliga påföljder och skydda

andra personers rättigheter och friheter. Inrättandet av databasen och den planerade behandlingen kan bidra till identifieringen av barn som förts bort mot sin vilja och kan därför betraktas som en lämplig åtgärd för att stödja det legitima målet att utreda och lagföra sådana brott.

Databasens ändamål och införandet av uppgifter

Behandlingens ändamål fastställs tydligt i lagstiftningen. Databasen får endast användas för att identifiera försvunna barn som misstänks ha förts bort mot sin vilja och för vilka en brottsutredning har inletts under tillsyn av en rättslig myndighet och en anmälan om bortförande av barn har utfärdats. De villkor som fastställs i lagstiftningen för införandet av uppgifter i databasen syftar till att kraftigt begränsa antalet registrerade och mängden personuppgifter i databasen. Den person som har föräldraansvar över barnet måste informeras om den behandling som utförts och om villkoren för utövandet av barnets rättigheter i förhållande till den biometriska behandling som planeras i identifieringssyfte eller till de personuppgifter om barnet som lagras i databasen.

2.4. Slutsats

Eftersom den planerade behandlingen är nödvändig och proportionerlig, och eftersom det ligger i barnets bästa intresse att behandlingen av personuppgifter utförs, förutsatt att det finns tillräckliga garantier för att säkerställa utövandet av den registrerades rättigheter, särskilt med beaktande av att det är uppgifter om barn som behandlas, kan denna tillämpning av ansiktsigenkänning sannolikt anses vara förenlig med unionsrätten.

Med tanke på typen av behandling och den teknik som används, vilken medför en hög risk för den berörda registrerades rättigheter och friheter, anser EDPB dessutom att utarbetandet av ett förslag till en lagstiftningsåtgärd som ska antas av ett nationellt parlament eller av en regleringsåtgärd som grundar sig på en sådan lagstiftningsåtgärd som rör den planerade behandlingen, måste föregås av ett samråd med tillsynsmyndigheten för att säkerställa konsekvens och överensstämmelse med den tillämpliga rättsliga ramen (se artikel 28.2 i brottsdatadirektivet).

3 SCENARIO 3

3.1. Beskrivning

Under polisinsatser vid upplopp och i samband med efterföljande utredningar har ett antal personer identifierats som misstänkta, t.ex. genom tidigare utredningar med hjälp av övervakningskameror eller vittnen. Bilder av dessa misstänkta personer jämförs med bilder av personer som registrerats med övervakningskameror eller mobila enheter på eller i närheten av en brottsplats.

För att stärka bevisningen mot personer som misstänks ha deltagit i upplopp i samband med en demonstration inrättar polisen en databas bestående av bildmaterial som har en lös lokal och tidsmässig koppling till uppploppen. Databasen innehåller privata bilder som skickats till polisen av medborgare, material från övervakningskameror i kollektivtrafiken, filmer från polisens egen videoövervakning samt material som publicerats av media utan någon särskild begränsning eller skyddsåtgärd. Uppvisande av allvarligt brottsligt beteende är inte något villkor för insamlingen av filerna i databasen. Den innehåller således material om personer som inte var inblandade i uppploppen, däribland en betydande andel av lokalbefolkningen som råkade gå förbi vid tidpunkten för demonstrationen eller som deltog i demonstrationen men inte i uppploppen. Materialet omfattar tusentals video- och bildfiler.

Med hjälp av programvara för ansiktsigenkänning får alla ansikten som visas i dessa filer en unik identifieringskod. De misstänktas ansikten jämförs sedan automatiskt med dessa identifieringskoder.

Alla biometriska mallar i de tusentals video- och bildfilerna lagras i databasen tills alla eventuella utredningar har avslutats. Positiva matchningar hanteras av ansvariga tjänstemän, som sedan beslutar om ytterligare åtgärder. Det kan handla om att överföra den fil som finns i databasen till den berörda personens brottsregister samt ytterligare åtgärder, till exempel att personen förhörs eller grips.

I den nationella lagstiftningen finns en allmän bestämmelse, enligt vilken behandling av biometriska uppgifter i syfte att unikt identifiera en fysisk person är tillåten om det är absolut nödvändigt och under förutsättning att lämpliga skyddsåtgärder har vidtagits för den berörda personens rättigheter och friheter.

Uppgiftskälla:

- Typer av registrerade: ☒ Alla personer
- Bildkälla: ☒ Allmänt tillgängliga platser ☒ Privat aktör ☒ Andra fysiska personer ☒ Annan: media
- Koppling till brott: ☒ Inte nödvändigtvis direkt geografisk eller tidsmässig koppling
- Metod för inhämtning av uppgifter: ☒ På distans
- Sammanhang – påverkar andra grundläggande rättigheter: Ja, närmare bestämt ☒ mötesfriheten
- Andra tillgängliga källor till information om den registrerade:
  ☒ Övriga: ej uteslutet (t.ex. användning av bankomater eller besökta butiker), eftersom ingen kontroll får utövas över motiv i bilder

Referensdatabas (mot vilken inhämtade uppgifter jämförs):

- Typ: ☒ Särskilda databaser med anknytning till brottsområdet

Algoritm:

- Typ av behandling: ☒ En mot många-identifiering

Resultat:

- Inverkan: ☒ Direkt (t.ex. den registrerade kan komma att gripas eller förhöras)
- Automatiserat beslut: ☒ NEJ
- Lagringstid: till dess att alla eventuella utredningar har avslutats

Rättslig analys:

- Typ av förhandsinformation till den registrerade: ☒ På den brottsbekämpande myndighetens allmänna webbplats
- Tillämplig rättslig ram: ☒ Brottsdatadirektivet till största delen kopierad till nationell lagstiftning ☒ Allmän nationell lagstiftning för brottsbekämpande myndigheters användning av biometriska uppgifter

3.2. Tillämplig rättslig ram

Som förklaras ovan är rättsliga grunder som endast upprepar den allmänna klausulen i artikel 10 i brottsdatadirektivet inte tillräckligt tydliga för att ge enskilda personer kännedom om de villkor och omständigheter under vilka brottsbekämpande myndigheter har befogenhet att använda inspelningar från övervakningskameror på offentliga platser för att skapa biometriska mallar av personernas ansikten och jämföra dem med polisdatabaser, andra tillgängliga övervakningskameror, privata inspelningar osv. Den rättsliga ram som fastställs i detta scenario uppfyller därför inte minimikraven för att fungera som rättslig grund.

3.3. Nödvändighet och proportionalitet

I detta exempel ger behandlingen av flera skäl upphov till farhågor kring nödvändighets- och proportionalitetsprinciperna, närmare bestämt följande:

Personerna är inte misstänkta för ett allvarligt brott. Uppvisande av allvarligt brottsligt beteende är inte något villkor för att filerna i den databas som innehåller bildmaterialet ska få användas. En direkt tidsmässig och geografisk koppling till brottet är inte heller ett villkor för att filerna i databasen ska få användas. Detta leder till att en betydande andel av lokalbefolkningen lagras i en biometrisk databas under en period som kan uppgå till flera år, fram till dess att alla utredningar har avslutats.

Brottsplatsdatabasen är inte begränsad till bilder som uppfyller proportionalitetskraven, vilket leder till ett obegränsat antal bilder som ska jämföras. Detta strider mot principen om uppgiftsminimering. En mindre mängd bilder skulle göra det möjligt att överväga icke-algoritmiska och mindre inkräktande metoder, t.ex. så kallade superigenkännare[88].

Eftersom exemplet är hämtat från en protestaktion är det även troligt att bilderna avslöjar deltagarnas politiska åsikter, vilket innebär att ytterligare en särskild kategori av uppgifter kan påverkas i detta scenario. Det framgår inte i scenariot hur insamlingen av dessa uppgifter kan förhindras och vilka skyddsåtgärder som kan vidtas. Om registrerade personer får veta att deras deltagande i en demonstration har lett till att de registrerats i en polisdatabas med biometriska uppgifter kan detta dessutom få allvarliga avskräckande effekter på deras framtida utövande av rätten till mötesfrihet.

De biometriska mallarna i databasen kan också jämföras med varandra. Detta gör det möjligt för polisen att inte bara söka efter en viss person i allt sitt material, utan även att återskapa en persons beteendemönster under en period på flera dagar. Polisen kan även samla in ytterligare information om personerna, till exempel sociala kontakter och politiskt engagemang.

Intrånget förstärks ytterligare av att uppgifterna behandlas utan de registrerades vetskap.

Med tanke på att människor i dag ständigt fångas på fotografier och videofilmer, och att de allestädes närvarande övervakningskamerorna också kan analyseras biometriskt, kan detta leda till allvarliga avskräckande effekter.

Den omfattande användningen av privata fotografier och videofilmer är en annan källa till farhågor, till exempel när det gäller risken för angiveri. Angiveri och annat missbruk är en risk i straffrättsliga förfaranden i allmänhet, men i detta fall är risken betydligt högre med tanke på den stora mängd uppgifter som behandlas och antalet personer som berörs. Det är inte otänkbart att material laddas upp för att sätta dit ovänner eller motståndare. Begäranden från polisen om att ladda upp fotografier och videofilmer kan leda till mycket låga trösklar för att personer ska tillhandahålla material, särskilt om det är möjligt att göra det anonymt eller åtminstone utan att behöva identifiera sig på en polisstation.

3.4. Slutsats

I detta exempel finns det ingen särskild bestämmelse som skulle kunna fungera som rättslig grund. Även om det hade funnits en tillräcklig rättslig grund skulle kraven på nödvändighet och proportionalitet inte vara uppfyllda, vilket skulle leda till ett oproportionerligt intrång i den registrerades rätt till respekt för privatlivet och skydd av personuppgifter enligt stadgan.

[88] Dvs. personer med en extraordinär förmåga att känna igen ansikten. Se även *Face Recognition by Metropolitan Police Super-Recognisers*, 26.2.2016, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

4 SCENARIO 4

4.1. Beskrivning

Polisen genomför en metod för att identifiera misstänkta i samband med ett allvarligt brott som fångats på övervakningskameror genom retroaktiv ansiktsigenkänning. En polistjänsteman väljer manuellt ut bilder av misstänkta personer i videomaterial som har inhämtats från brottsplatsen eller någon annan plats inom ramen för förundersökningen och skickar sedan bilderna till den kriminaltekniska avdelningen. Den kriminaltekniska avdelningen använder ansiktsigenkänningsteknik för att matcha dessa bilder mot bilder av individer som tidigare har samlats in i en databas (en så kallad beskrivningsdatabas som består av misstänkta och tidigare dömda personer). Under detta förfarande analyseras beskrivningsdatabasen – tillfälligt och i en isolerad miljö – med ansiktsigenkänningsteknik för att polisen ska kunna utföra matchningsprocessen. För att minimera ingreppet i de matchade personernas rättigheter och intressen har ett mycket begränsat antal anställda vid den kriminaltekniska avdelningen tillstånd att genomföra det faktiska matchningsförfarandet. Endast de tjänstemän som arbetar med det specifika ärendet har tillgång till uppgifterna, och en manuell kontroll av resultaten utförs innan något resultat vidarebefordras till den utredande tjänstemannen. De biometriska uppgifterna överförs inte utanför den kontrollerade och isolerade miljön. Endast resultatet och bilden (inte den biometriska mallen) används i den fortsatta utredningen. De anställda får särskild utbildning om reglerna och förfarandena för denna behandling, och all behandling av personuppgifter och biometriska uppgifter är tillräckligt specificerad i den nationella lagstiftningen.

Uppgiftskälla:

- Typer av registrerade: ☒ Misstänkta som identifierats med hjälp av övervakningskameror
- Bildkälla: ☒ Allmänt tillgängliga platser ☒ Internet
- Koppling till brott: ☒ Direkt tidsmässig
  ☒ Direkt geografisk
- Metod för inhämtning av uppgifter: ☒ På distans
- Sammanhang – påverkar andra grundläggande rättigheter: Ja, närmare bestämt ☒ mötesfriheten ☒ yttrandefriheten ☒ övriga: __

Referensdatabas (mot vilken inhämtade uppgifter jämförs):

- Typ: ☒ Särskilda databaser med anknytning till brottsområdet

Algoritm:

- Typ av behandling: ☒ En mot många-identifiering

Resultat:

- Inverkan: ☒ Direkt (t.ex. den registrerade grips eller förhörs)
- Automatiserat beslut: ☒ NEJ

Rättslig analys:

- Tillämplig rättslig ram: ☒ Särskild nationell lagstiftning för denna behandling (ansiktsigenkänning) för den behöriga myndigheten

4.2. Tillämplig rättslig ram

I detta scenario anges i den nationella lagstiftningen att biometriska uppgifter får användas för att utföra en kriminalteknisk analys om det är absolut nödvändigt för att uppnå syftet, dvs. att identifiera personer som misstänks ha begått ett allvarligt brott genom att matcha bilderna i

beskrivningsdatabasen. I den nationella lagstiftningen anges vilka uppgifter som får behandlas, liksom förfarandena för att bevara personuppgifternas integritet och konfidentialitet samt förfarandena för att förstöra dem. Detta ger därför tillräckliga garantier mot risken för missbruk och godtycklighet.

4.3. Nödvändighet och proportionalitet

Användningen av ansiktsigenkänning är mer tidseffektiv än manuell matchning på kriminalteknisk nivå. Det manuella urvalet av bilder i förväg begränsar intrånget jämfört med om allt videomaterial hade jämförts mot en databas. Behandlingen är därmed endast riktad mot de personer som omfattas av målet, dvs. att bekämpa grov brottslighet. Det är emellertid fortfarande viktigt att överväga om matchningen kan göras manuellt inom rimlig tid, beroende på det aktuella fallet. Inverkan på rätten till privatliv och dataskydd begränsas, eftersom endast ett fåtal personer har tillgång till tekniken och personuppgifterna och eftersom de biometriska mallarna inte lagras eller används senare i utredningen. Den manuella kontrollen av resultatet innebär även en minskad risk för falska positiva resultat.

4.4. Slutsats

Det är viktigt att den nationella lagstiftningen utgör en lämplig rättslig grund för behandlingen av biometriska uppgifter och för matchningen mot den nationella databasen. I detta scenario har flera åtgärder vidtagits för att begränsa intrånget i rätten till dataskydd, däribland de villkor för användningen av ansiktsigenkänningsteknik som anges i den rättsliga grunden, antalet personer som har tillgång till tekniken och de biometriska uppgifterna, de manuella kontrollerna osv. Ansiktsigenkänningstekniken ökar effektiviteten i det utredningsarbete som utförs av polisens kriminaltekniska avdelning och bygger på lagstiftning som gör att polisen kan behandla biometriska uppgifter när det är absolut nödvändigt, vilket i detta sammanhang kan anses vara ett lagligt intrång i den enskildes rättigheter.

5 SCENARIO 5

5.1. Beskrivning

Biometrisk fjärridentifiering används på offentliga platser för att fastställa personers identitet på distans med hjälp av biometriska kännetecken (ansiktsbild, gångstil, regnbågshinna osv.) som kontrolleras kontinuerligt mot (biometriska) uppgifter i en databas[89]. Biometrisk fjärridentifiering utförs i realtid om upptagningen av bildmaterialet, jämförelsen och identifieringen sker utan betydande dröjsmål.

Innan biometrisk fjärridentifiering i realtid börjar användas sammanställer polisen en bevakningslista över personer som kan vara intressanta i en utredning. Listan fylls med ansiktsbilder av de olika personerna. Baserat på underrättelser som antyder att personerna kommer att befinna sig i ett visst område, t.ex. i ett köpcenter eller på ett torg, beslutar polisen när, var och hur länge den biometriska fjärridentifieringen ska användas.

På dagen för insatsen placeras en skåpbil ut som kontrollcentral, med en högre polistjänsteman närvarande. I skåpbilen finns bildskärmar som visar bilder från övervakningskameror i närheten, vilka antingen har installerats särskilt för ändamålet eller anslutits till videoströmmar från redan installerade kameror. När fotgängare passerar förbi kamerorna används tekniken för att ta ansiktsbilder, omvandla dem till biometriska mallar och jämföra dem med personerna i bevakningslistan.

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

Om en potentiell matchning upptäcks mellan bevakningslistan och de som passerar kamerorna skickas en varning till poliserna i skåpbilen, som sedan informerar poliserna på fältet om varningen är positiv, t.ex. via radioutrustning. Den polis som får uppdraget beslutar sedan om han eller hon ska ingripa, ta kontakt med eller gripa personen. Alla åtgärder som vidtas av polisen registreras. Vid en diskret kontroll lagras de uppgifter som samlas in (t.ex. vem personen är tillsammans med, vilka kläder de har på sig och vart de är på väg).

I den nationella lagstiftning som det hänvisas till finns en allmän bestämmelse, enligt vilken behandling av biometriska uppgifter i syfte att unikt identifiera en fysisk person är tillåten om det är absolut nödvändigt och under förutsättning att lämpliga skyddsåtgärder har vidtagits för den berörda personens rättigheter och friheter.

Uppgiftskälla:

- Typer av registrerade: ☒ Alla personer
- Bildkälla: ☒ Allmänt tillgängliga platser
- Koppling till brott: ☒ Inte nödvändigtvis direkt geografisk eller tidsmässig koppling
- Metod för inhämtning av uppgifter: ☒ På distans
- Sammanhang – påverkar andra grundläggande rättigheter: Ja, närmare bestämt ☒ mötesfriheten ☒ yttrandefriheten ☒ övriga
- Andra tillgängliga källor till information om den registrerade:
  ☒ Övriga: ej uteslutet (t.ex. användning av bankomater eller besökta butiker)

Referensdatabas (mot vilken inhämtade uppgifter jämförs):

- Typ: ☒ Särskilda databaser med anknytning till brottsområdet

Algoritm:

- Typ av behandling: ☒ En mot många-identifiering

Resultat:

- Inverkan: ☒ Direkt (t.ex. den registrerade grips eller förhörs)
- Automatiserat beslut: ☒ NEJ
- Lagringstid: till dess att alla eventuella utredningar har avslutats

Rättslig analys:

- Typ av förhandsinformation till den registrerade: ☒ På den brottsbekämpande myndighetens allmänna webbplats
- Tillämplig rättslig ram: ☒ Brottsdatadirektivet till största delen kopierad till nationell lagstiftning ☒ Allmän nationell lagstiftning för brottsbekämpande myndigheters användning av biometriska uppgifter

5.2. Tillämplig rättslig ram

Rättsliga grunder som endast upprepar den allmänna klausulen i artikel 10 i brottsdatadirektivet är inte tillräckligt tydliga för att ge enskilda personer kännedom om de villkor och omständigheter under vilka brottsbekämpande myndigheter har befogenhet att använda inspelningar från övervakningskameror på offentliga platser för att skapa biometriska mallar av personernas ansikten

och jämföra dem med polisdatabaser. Den rättsliga ram som fastställs i detta scenario uppfyller därför inte minimikraven för att fungera som rättslig grund[90].

5.3. Nödvändighet och proportionalitet

Kraven på nödvändighet och proportionalitet blir högre ju mer omfattande intrånget är. Biometrisk fjärridentifiering på offentliga platser medför flera konsekvenser för de grundläggande rättigheterna:

Scenarierna innebär övervakning av alla förbipasserande på de respektive offentliga platserna. Tekniken har därför en betydande inverkan på befolkningens rimliga förväntning att vara anonym på offentliga platser[91]. Detta är en förutsättning för många aspekter av den demokratiska processen, däribland beslutet att ansluta sig till en medborgarförening, delta i sammankomster och träffa människor med olika social och kulturell bakgrund, delta i politiska protester och besöka platser av skilda slag. Anonymiteten på offentliga platser är avgörande för möjligheten att fritt kunna inhämta och utbyta information och idéer. Den bidrar till att bevara åsiktsfriheten, friheten att delta i fredliga sammankomster, föreningsfriheten och skyddet av minoriteter, samtidigt som den stöder principerna om maktfördelning och kontroller och motvikter. Om anonymiteten på offentliga platser undergrävs kan det leda till en allvarlig avskräckande effekt. Medborgarna kan komma att avstå från vissa beteenden som ligger inom ramen för ett fritt och öppet samhälle. Detta skulle påverka allmänintresset, eftersom ett demokratiskt samhälle kräver att medborgarna har rätt till självbestämmande och deltagande i den demokratiska processen.

Om sådan teknik används kommer de brottsbekämpande myndigheterna att samla in uppgifter, däribland biometriska uppgifter, om personer som bara promenerar längs trottoarerna, till tunnelbanan eller till bageriet i det berörda området och, i det första scenariot, även matcha dem mot polisdatabaser. En situation där samma sak görs genom att ta fingeravtryck skulle vara uppenbart oproportionerlig.

Antalet registrerade som påverkas är extremt högt, eftersom alla som befinner sig i det offentliga området registreras. Dessutom skulle scenarierna innebära automatisk massbehandling av biometriska uppgifter och massmatchning av biometriska uppgifter mot polisdatabaser.

Enligt europeisk rättspraxis är massövervakning förbjuden (t.ex. ansåg Europeiska domstolen för de mänskliga rättigheterna i målet S. och Marper mot Förenade kungariket att den godtyckliga lagringen av biometriska uppgifter utgjorde ett oproportionerligt intrång i rätten till privatliv, eftersom den inte kan anses vara nödvändig i ett demokratiskt samhälle).

Biometrisk fjärridentifiering är så nära förknippad med massövervakning att det inte finns några tillförlitliga sätt att begränsa den. Tekniken skiljer sig väsentligen från videoövervakning, eftersom användningen av ansiktsigenkänningsteknik förändrar kvaliteten hos det utbredda videoövervakningssystem som är den huvudsakliga källan till uppgifterna, medan användningen av videofilmer utan biometrisk identifiering medför ett begränsat intrång, även om det i sig är allvarligt. Med tanke på de avskräckande effekterna kommer eventuella begränsningar i tillämpningen av de redan befintliga videoövervakningskamerorna inte att vara synliga och därmed inte betrodda av allmänheten.

[90] Om personuppgifter måste behandlas i samband med ett vetenskapligt projekt som syftar till att undersöka användningen av ansiktsigenkänningsteknik, och om den behandlingen inte omfattas av artikel 4.3 i brottsdatadirektivet eller av unionsrätten, är den allmänna dataskyddsförordningen tillämplig. När det gäller pilotprojekt som följs av brottsbekämpande insatser är det brottsdatadirektivet som tillämpas.

[91] EDPB:s svar till Europaparlamentets ledamöter angående den app för ansiktsigenkänning som utvecklats av Clearview AI, 10 juni 2020, ref: OUT2020-0052.

Polismyndigheter som använder biometrisk fjärridentifiering behandlar alla personer som möjliga misstänkta. I en rättsstat förutsätts emellertid att alla medborgare är oskyldiga tills motsatsen bevisats. Denna princip återspeglas även delvis i brottsdatadirektivet, som understryker behovet att i möjligaste mån skilja mellan behandlingen av brottsoffer och misstänkta där brottsbekämpande myndigheter måste ha ”tungt vägande skäl att anta att de har begått eller är på väg att begå ett brott” (artikel 6 a i brottsdatadirektivet) jämfört med personer som inte har dömts eller inte misstänks för brottslig verksamhet.

Om brottsbekämpande myndigheter använder en teknik som unikt kan identifiera en enskild person samt spåra och analysera personens vistelseort och rörelser vid transportknutpunkter eller på offentliga platser kommer den även att avslöja vissa av personens mest känsliga uppgifter (t.ex. sexuell läggning, religion och hälsoproblem). Samtidigt tillkommer den enorma risken för olaglig tillgång till och användning av uppgifterna.

Installationen av ett system som gör det möjligt att avslöja själva kärnan i den enskilda personens beteenden och egenskaper leder till starka avskräckande effekter. Det kan få människor att ifrågasätta om de ska gå med i en viss manifestation och skadar därmed den demokratiska processen. Att träffa och synas offentligt med en vän som är känd av polisen eller beter sig på ett unikt sätt kan också ses som kritiskt, eftersom allt detta skulle påverka systemets algoritm och därmed brottsbekämpningen.

Det är omöjligt att skydda barn och andra sårbara registrerade personer. Dessutom påverkas personer som har ett yrkesmässigt intresse – och ofta en motsvarande rättslig skyldighet – att hålla sina kontakter konfidentiella, till exempel journalister, advokater och präster. Detta kan t.ex. leda till avslöjandet att en journalist varit i kontakt med en uppgiftslämnare eller att en person har anlitat en brottmålsadvokat. Problemet gäller inte bara slumpmässiga offentliga platser, t.ex. där journalister och deras uppgiftslämnare möts, utan även offentliga platser där institutioner eller yrkesverksamma är verksamma.

Dessutom kan människors obehag inför ansiktsigenkänningstekniken leda till att de ändrar sitt beteende, undviker platser där tekniken används och därmed håller sig borta från det sociala och kulturella livet. Beroende på omfattningen av införandet av ansiktsigenkänningsteknik kan konsekvenserna för människor vara så stora att de påverkar deras möjlighet att leva ett värdigt liv[92].

Det är därför högst sannolikt att det väsentliga innehållet – den okränkbara kärnan – i rätten till skydd av personuppgifter kommer att påverkas. Starka indikationer på detta (se avsnitt 3.1.3.2 i riktlinjerna) är i synnerhet följande: Brottsbekämpande myndigheter behandlar människors unika biologiska egenskaper automatiskt och i stor skala med algoritmer baserade på rimlighet som har en begränsad förklarbarhet. Begränsningar av rätten till privatliv och dataskydd införs oberoende av personens eget beteende eller de omständigheter som rör honom eller henne. Statistiskt sett är nästan alla registrerade som påverkas av intrånget laglydiga personer. Det finns endast begränsade möjligheter att informera den registrerade. I de flesta fall kommer rättslig prövning att vara möjlig först i ett senare skede.

Användningen av ett system som bygger på rimlighet och som har begränsad förklarbarhet kan leda till ansvarsspridning, orsaka en brist på korrigerande åtgärder och vara ett incitament till försumlighet.

Ett sådant system kan även tillämpas på befintliga övervakningskameror, och när det väl har införts kan det med mycket liten ansträngning och utan att vara synligt för enskilda personer missbrukas och

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

användas för att snabbt och systematiskt upprätta listor över personer efter etniskt ursprung, kön, religion osv. Principen att behandla personuppgifter mot bakgrund av förutbestämda kriterier, såsom en persons vistelseort och resväg, praktiseras redan[93] och kan leda till diskriminering.

Med tanke på känsligheten, den avslöjande karaktären och mängden behandlade uppgifter finns det risk för att system för ansiktsigenkänning på distans på allmänt tillgängliga platser missbrukas, med skadliga effekter för de berörda personerna. Uppgifterna kan även lätt samlas in och missbrukas för att sätta press på aktörer enligt principen om kontroller och motvikter, till exempel politiska motståndare, tjänstemän och journalister.

Slutligen har ansiktsigenkänningssystem en tendens att medföra en stark snedvridning när det gäller ras och kön. Icke-vita och kvinnor påverkas oproportionerligt mycket av falska positiva resultat[94],vilket leder till diskriminering. Polisens åtgärder efter ett falskt positivt resultat, däribland husrannsakningar och gripanden, stigmatiserar dessa grupper ytterligare.

5.4. Slutsats

De ovannämnda scenarierna avseende fjärrbehandling av biometriska uppgifter på offentliga platser i identifieringssyfte medför inte en rättvis jämvikt mellan de konkurrerande privata och allmänna intressena och utgör därmed ett oproportionerligt intrång i den registrerades rättigheter enligt artiklarna 7 och 8 i stadgan.

6 SCENARIO 6

6.1. Beskrivning

En privat aktör tillhandahåller ett program där ansiktsbilder ”skrapas” från internet för att skapa en databas. Användaren, t.ex. polisen, kan sedan ladda upp en bild och med hjälp av biometrisk identifiering försöka matcha den med ansiktsbilder eller biometriska mallar i sin databas.

En lokal polismyndighet utreder ett brott som fångats på film där ett antal potentiella vittnen och misstänkta inte kan identifieras genom att matcha insamlade uppgifter med interna databaser eller underrättelser. De insamlade uppgifterna visar att personerna inte är registrerade i någon befintlig polisdatabas. Polisen beslutar sig för att använda det verktyg som beskrivs ovan, som tillhandahålls av ett privat företag, för att identifiera enskilda personer genom biometrisk identifiering.

Uppgiftskälla:

- Typer av registrerade: ☒ Alla medborgare (vittnen) ☒ Dömda brottslingar ☒ Misstänkta personer
- Bildkälla: ☒ Videomaterial från en offentlig plats eller filmer som inhämtats på någon annan plats inom ramen för en förundersökning
- Koppling till brott: ☒ Ej nödvändig
- Metod för inhämtning av uppgifter: ☒ På distans

[93] Se artikel 6 i Europaparlamentets och rådets direktiv (EU) 2016/681 av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet och artikel 33 i Europaparlamentets och rådets förordning (EU) 2018/1240 av den 12 september 2018 om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) och om ändring av förordningarna (EU) nr 1077/2011, (EU) nr 515/2014, (EU) 2016/399, (EU) 2016/1624 och (EU) 2017/2226.
[94] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

- Sammanhang – påverkar andra grundläggande rättigheter: Ja, närmare bestämt: ☒ mötesfriheten ☒ yttrandefriheten ☒ övriga: __

Referensdatabas (mot vilken inhämtade uppgifter jämförs):

- Typ: ☒ Databaser för allmänna ändamål med uppgifter som hämtats från internet

Algoritm:

- Typ av behandling: ☒ En mot många-identifiering

Resultat:

- Inverkan: ☒ Direkt (t.ex. den registrerade grips, förhörs, utsätts för diskriminerande beteende)
- Automatiserat beslut: ☒ NEJ

Rättslig analys:

- Typ av förhandsinformation till den registrerade: ☒ Ingen

6.2. Tillämplig rättslig ram

När en privat aktör tillhandahåller en tjänst som omfattar behandling av personuppgifter för vilken aktören bestämmer ändamål och medel (i detta fall att skrapa bilder från internet för att skapa en databas) måste den privata aktören ha en rättslig grund för denna behandling. Vidare måste den brottsbekämpande myndighet som beslutar sig för att använda denna tjänst för sina ändamål ha en rättslig grund för behandlingen och dess ändamål och medel. För att den brottsbekämpande myndigheten ska få behandla biometriska uppgifter måste det finnas en rättslig ram som specificerar syftet med behandlingen, vilka personuppgifter som ska behandlas, behandlingens ändamål samt förfarandena för att bevara personuppgifternas integritet och konfidentialitet och förfarandena för att förstöra uppgifterna.

Detta scenario innebär en omfattande insamling av personuppgifter från enskilda personer som inte är medvetna om att deras uppgifter samlas in. Sådan behandling kan endast vara laglig under mycket exceptionella omständigheter. Beroende på var databasen finns kan användningen av tjänsten innebära att personuppgifter och/eller särskilda kategorier av personuppgifter överförs till en plats utanför Europeiska unionen (av polisen, t.ex. genom att skicka en ansiktsbild som hämtats från en övervakningsvideo eller som inhämtats på annat sätt), vilket kräver särskilda villkor för överföringen (se artikel 39 i brottsdatadirektivet).

Det finns inga särskilda regler i detta scenario som ger den brottsbekämpande myndigheten tillstånd för behandlingen.

6.3. Nödvändighet och proportionalitet

Den brottsbekämpande myndighetens användning av tjänsten innebär att personuppgifter delas med en privat aktör som använder en databas där personuppgifter samlas in på ett obegränsat och storskaligt sätt. Det finns inget samband mellan de personuppgifter som samlas in och det mål som den brottsbekämpande myndigheten eftersträvar. Den brottsbekämpande myndighetens utbyte av uppgifter med den privata aktören gör även att myndigheten inte har kontroll över de uppgifter som behandlas av den privata aktören och att de registrerade får svårt att utöva sina rättigheter, eftersom de inte är medvetna om att deras uppgifter behandlas på detta sätt. Tröskeln för situationer där en sådan behandling skulle kunna genomföras är följaktligen mycket hög. Det är tveksamt om något mål skulle uppfylla de krav som anges i direktivet, eftersom alla undantag från och begränsningar av rätten till privatliv och dataskydd endast är tillämpliga när det är absolut nödvändigt. Det allmänna samhällsintresset av en effektiv kamp mot allvarlig brottslighet kan inte i sig motivera en behandling

där så stora mängder uppgifter samlas in utan åtskillnad. Denna behandling skulle därför inte uppfylla kraven på nödvändighet och proportionalitet.

6.4. Slutsats

Avsaknaden av tydliga, exakta och förutsägbara regler som uppfyller kraven i artiklarna 4 och 10 i direktivet, och avsaknaden av bevis för att denna behandling är absolut nödvändig för att uppnå de avsedda målen, leder till slutsatsen att användningen av programmet inte skulle uppfylla kraven på nödvändighet och proportionalitet, utan innebära ett oproportionerligt intrång i de registrerades rätt till respekt för privatlivet och skydd av personuppgifter enligt stadgan.