Translations proofread by EDPB Members.

This language version has not yet been proofread.

Richtsnoeren 05/2022 voor het gebruik van gezichtsherkenningstechnologie in het kader van rechtshandhaving

Versie 2.0

Vastgesteld op 26 april 2023

Versiegeschiedenis

Versie 1.0	12 mei 2022	Vaststelling van de richtsnoeren voor openbare raadpleging
Versie 2.0	26 april 2023	Vaststelling van de richtsnoeren na openbare raadpleging

Inhoudsopgave

SAMENVATTING

Steeds meer rechtshandhavingsinstanties passen gezichtsherkenningstechnologie toe of zijn voornemens deze toe te passen. De technologie kan worden gebruikt om een persoon te **authenticeren** of te **identificeren** en kan voor video's (bijv. CCTV) of foto's worden ingezet, maar ook voor andere doeleinden, waaronder het opzoeken van personen op signaleringslijsten van de politie of het volgen van de bewegingen van een persoon in de openbare ruimte.

Gezichtsherkenningstechnologie is gebaseerd op de verwerking van **biometrische gegevens** en omvat derhalve de verwerking van bijzondere categorieën persoonsgegevens. Vaak wordt bij gezichtsherkenningstechnologie gebruikgemaakt van componenten van **artificiële intelligentie** of machinaal leren. Hoewel hierdoor gegevensverwerking op grote schaal mogelijk wordt, brengt het ook het risico van discriminatie en foutieve resultaten met zich mee. Gezichtsherkenningstechnologie kan worden gebruikt in gecontroleerde één-op-éénsituaties, maar ook voor grote menigten en belangrijke vervoersknooppunten.

Gezichtsherkenningstechnologie is een **gevoelig instrument voor rechtshandhavingsinstanties**. Rechtshandhavingsinstanties zijn uitvoerende autoriteiten en hebben soevereine bevoegdheden. Gezichtsherkenningstechnologie staat op gespannen voet met de grondrechten, waarbij meer dan alleen de bescherming van persoonsgegevens op het spel staat, en kan onze sociale en democratische politieke stabiliteit aantasten.

Voor de bescherming van persoonsgegevens in het kader van rechtshandhaving moet aan de **vereisten van de richtlijn gegevensbescherming bij rechtshandhaving** (hierna de "RGR" genoemd) worden voldaan. De richtlijn gegevensbescherming bij rechtshandhaving voorziet in een bepaald raamwerk voor het gebruik van gezichtsherkenningstechnologie, met name in artikel 3, lid 13 (term "biometrische gegevens"), artikel 4 (beginselen inzake verwerking van persoonsgegevens), artikel 8 (rechtmatigheid van de verwerking), artikel 10 (verwerking van bijzondere categorieën van persoonsgegevens) en artikel 11 (geautomatiseerde individuele besluitvorming) van de RGR.

Ook verscheidene andere grondrechten kunnen worden aangetast door de toepassing van gezichtsherkenningstechnologie. Daarom is het **Handvest van de grondrechten van de EU** ("het Handvest") van essentieel belang voor de interpretatie van de richtlijn gegevensbescherming bij rechtshandhaving, in het bijzonder het recht op bescherming van persoonsgegevens in artikel 8 van het Handvest, maar ook het in artikel 7 van het Handvest vastgelegde recht op eerbiediging van het privéleven.

Wetgevingsmaatregelen die dienen als rechtsgrondslag voor de verwerking van persoonsgegevens, vormen een rechtstreekse inmenging in de rechten die worden gewaarborgd door de artikelen 7 en 8 van het Handvest. Het onder alle omstandigheden verwerken van biometrische gegevens vormt een ernstige inmenging op zich. Dit staat los van de uitkomst, zoals een positieve match. Beperkingen op de uitoefening van grondrechten en vrijheden moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen.

De formulering van de rechtsgrondslag moet **voldoende duidelijk** zijn om burgers een adequate indicatie te geven van de voorwaarden waaronder en de omstandigheden waarin overheidsdiensten bevoegd zijn om maatregelen te nemen op het gebied van gegevensverzameling en geheime observatie. Bij een loutere omzetting in nationaal recht van de algemene bepaling in artikel 10 RGR zou er sprake zijn van een gebrek aan precisie en voorspelbaarheid.

Voordat de nationale wetgever een nieuwe rechtsgrondslag voor enige vorm van verwerking van biometrische gegevens met behulp van gezichtsherkenning creëert, moet de bevoegde toezichthoudende autoriteit voor gegevensbescherming worden **geraadpleegd**.

Wetgevingsmaatregelen moeten **passend** zijn voor het verwezenlijken van de legitieme doelstellingen die met de wetgeving in kwestie worden nagestreefd. Een **doelstelling van algemeen belang**, hoe fundamenteel ook, rechtvaardigt op zich niet een beperking van een grondrecht. De wetgevingsmaatregelen moeten **onderscheid maken** tussen en gericht zijn op personen die in het licht van de doelstelling, bijvoorbeeld de bestrijding van bepaalde ernstige strafbare feiten, onder de richtlijn vallen. Als de maatregel algemeen van toepassing is op alle personen zonder dat er sprake is van een dergelijk onderscheid of een dergelijke beperking of uitzondering, wordt de inmenging versterkt. De maatregel leidt tot een nog sterkere inmenging als de gegevensverwerking betrekking heeft op een aanzienlijk deel van de bevolking.

De gegevens moeten worden verwerkt op een manier die de toepasbaarheid en doeltreffendheid van de gegevensbeschermingsregels en -beginselen in de Unie waarborgt. Op basis van elke situatie moeten bij de **beoordeling van de noodzakelijkheid en evenredigheid** ook alle mogelijke gevolgen voor andere grondrechten worden vastgesteld en in aanmerking worden genomen. Indien de gegevens systematisch worden verwerkt zonder dat de betrokkenen daarvan op de hoogte zijn, kan er een **algemeen gevoel ontstaan dat men voortdurend in de gaten wordt gehouden**. Dit kan een gevoel van angst opwekken met betrekking tot sommige of alle betrokken grondrechten, zoals de menselijke waardigheid uit hoofde van artikel 1 van het Handvest, de vrijheid van gedachte, geweten en godsdienst uit hoofde van artikel 10 van het Handvest, de vrijheid van meningsuiting uit hoofde van artikel 11 van het Handvest en de vrijheid van vergadering en vereniging uit hoofde van artikel 12 van het Handvest.

De verwerking van bijzondere categorieën gegevens, zoals biometrische gegevens, kan alleen als "**strikt noodzakelijk**" (artikel 10 RGR) worden aangemerkt als de inmenging in de bescherming van persoonsgegevens en de bijbehorende beperkingen beperkt blijft tot wat absoluut noodzakelijk, d.w.z. onontkoombaar, is en elke verwerking van algemene of systematische aard uitsluit.

Het feit dat een foto **kennelijk door de betrokkene zelf openbaar is gemaakt** (artikel 10 RGR) betekent niet dat de biometrische gegevens uit die foto, die met specifieke technische middelen kunnen worden opgeroepen, worden aangemerkt als kennelijk openbaar gemaakt. Standaardinstellingen van een dienst, bijv. het openbaar beschikbaar stellen van sjablonen of het ontbreken van een keuze, bijvoorbeeld doordat sjablonen openbaar worden gemaakt zonder dat de gebruiker deze instelling kan wijzigen, mogen op geen enkele manier worden uitgelegd als gegevens die kennelijk openbaar zijn gemaakt.

In artikel 11 RGR is een raamwerk voor **geautomatiseerde individuele besluitvorming** vastgesteld. Het gebruik van gezichtsherkenningstechnologie houdt het gebruik van bijzondere categorieën gegevens in en kan leiden tot profilering, afhankelijk van de manier waarop en het doel waarvoor gezichtsherkenningstechnologie wordt toegepast. In overeenstemming met het Unierecht en artikel 11, lid 3, RGR moet profilering die leidt tot discriminatie van natuurlijke personen op basis van bijzondere categorieën persoonsgegevens, in ieder geval verboden worden.

Artikel 6 RGR heeft betrekking op de noodzaak om **een onderscheid te maken tussen de verschillende categorieën betrokkenen**. Bij betrokkenen voor wie er geen bewijs is dat erop kan duiden dat er een verband, zelfs een indirect of gering verband, zou kunnen bestaan tussen het gedrag van de betrokkene en het legitieme doel zoals bepaald in de RGR, is er hoogstwaarschijnlijk geen rechtvaardiging voor inmenging.

Volgens het **beginsel van minimale gegevensverwerking** (artikel 4, lid 1, punt e), RGR) moet al het videomateriaal dat niet relevant is voor het doel van de verwerking altijd worden verwijderd of geanonimiseerd voordat het wordt gebruikt (bijv. door het onscherp te maken, zonder de mogelijkheid de gegevens later te herstellen).

Voordat er verwerking van gezichtsherkenningstechnologie plaatsvindt, moet de verwerkingsverantwoordelijke zorgvuldig nagaan hoe aan de vereisten voor **de rechten van betrokkenen** moet (of kan) worden voldaan. Bij de verwerking van gezichtsherkenningstechnologie is immers vaak sprake van verwerking van bijzondere categorieën persoonsgegevens zonder dat er een duidelijke interactie met de betrokkene bestaat.

De daadwerkelijke uitoefening van de rechten van betrokkenen is afhankelijk van de naleving door de verwerkingsverantwoordelijke van zijn of haar **informatieverplichtingen** (artikel 13 RGR). Bij de beoordeling van de vraag of er sprake is van een "specifiek geval" in de zin van artikel 13, lid 2, RGR, moeten verschillende factoren in aanmerking worden genomen, onder meer of de persoonsgegevens worden verzameld zonder dat de betrokkene hiervan op de hoogte is. Dit zou immers de enige manier zijn waarop betrokkenen doeltreffend hun rechten kunnen uitoefenen. Indien de besluitvorming uitsluitend op basis van gezichtsherkenningstechnologie plaatsvindt, moeten de betrokkenen worden geïnformeerd over de kenmerken van de geautomatiseerde besluitvorming.

Wat betreft **verzoeken om inzage**: wanneer biometrische gegevens ook door middel van alfanumerieke gegevens worden opgeslagen en aan een identiteit worden gekoppeld, overeenkomstig het beginsel van gegevensminimalisering, moet de bevoegde autoriteit een verzoek om inzage kunnen bevestigen op basis van een zoekopdracht aan de hand van die alfanumerieke gegevens, zonder verdere verwerking van biometrische gegevens van anderen (d.w.z. door met gezichtsherkenningstechnologie te zoeken in een database).

De risico's voor de betrokkenen zijn met name ernstig indien er onjuiste gegevens worden opgeslagen in een politiedatabase en/of worden gedeeld met andere entiteiten. De verwerkingsverantwoordelijke moet de opgeslagen gegevens en gezichtsherkenningstechnologiesystemen dienovereenkomstig **corrigeren** (zie ook overweging 47 RGR).

Het recht op **beperking** wordt met name belangrijk bij het gebruik van gezichtsherkenningstechnologie (die uitgaat van een of meer algoritmen en dus nooit een doorslaggevend resultaat laat zien) in situaties waarin grote hoeveelheden gegevens worden verzameld en de nauwkeurigheid en kwaliteit van de identificatie kunnen variëren.

Op grond van artikel 27 RGR is een **gegevensbeschermingseffectbeoordeling** of privacyeffectbeoordeling (PEB) een essentiële voorwaarde die moet worden vervuld voordat er gezichtsherkenningstechnologie wordt gebruikt. De EDPB beveelt aan om de resultaten van dergelijke beoordelingen, of ten minste de belangrijkste bevindingen en conclusies van de PEB, openbaar te maken als een maatregel ter bevordering van vertrouwen en transparantie.

In de meeste gevallen waarin gezichtsherkenningstechnologie wordt ingezet en gebruikt, is er een inherent hoog risico voor de rechten en vrijheden van betrokkenen. Om die reden moet de autoriteit die de gezichtsherkenningstechnologie inzet de bevoegde toezichthoudende autoriteit **raadplegen** voordat het systeem wordt ingezet.

Gezien het unieke karakter van biometrische gegevens moet de instantie die gezichtsherkenningstechnologie invoert en/of gebruikt, bijzondere aandacht besteden aan de **beveiliging van de verwerking** overeenkomstig artikel 29 van de richtlijn. De

rechtshandhavingsinstantie moet er met name voor zorgen dat het systeem voldoet aan de relevante normen en dat beschermingsmaatregelen voor de biometrische template zijn getroffen. De beginselen en waarborgen voor gegevensbescherming moeten zijn ingebed in de technologie voordat de verwerking van persoonsgegevens van start gaat. Daarom moet een rechtshandhavingsinstantie, ook wanneer deze voornemens is gezichtsherkenningstechnologie van externe aanbieders toe te passen en te gebruiken, ervoor zorgen dat alleen gezichtsherkenningstechnologie wordt ingezet die is ontwikkeld op basis van de beginselen van **gegevensbescherming door ontwerp en door standaardinstellingen**, bijvoorbeeld via de aanbestedingsprocedure.

Logbestanden (zie artikel 25 RGR) zijn een belangrijke waarborg voor de verificatie van de rechtmatigheid van de verwerking, zowel intern (d.w.z. interne controle door de betrokken verwerkingsverantwoordelijke/verwerker) als door externe toezichthoudende autoriteiten. In het kader van gezichtsherkenningssystemen wordt ook aanbevolen logbestanden bij te houden voor wijzigingen in de referentiedatabestanden en voor pogingen tot identificatie of verificatie die betrekking hebben op een gebruiker, resultaat en vertrouwensscore. Het bijhouden van logbestanden is echter slechts een van de essentiële elementen van het algemene **verantwoordingsbeginsel** (zie artikel 4, lid 4, RGR). De verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerking in overeenstemming is met de fundamentele gegevensbeschermingsbeginselen van artikel 4, leden 1 en 3, RGR.

De EDPB herinnert aan de gezamenlijk met de EDPS gedane **oproep voor een verbod** op bepaalde vormen van verwerking die verband houden met 1) biometrische identificatie op afstand van personen in openbare ruimten, 2) door AI ondersteunde gezichtsherkenningssystemen waarbij personen op basis van hun biometrische gegevens worden ingedeeld in clusters, zoals etnische afkomst, geslacht, politieke of seksuele oriëntatie of andere discriminatiegronden, 3) het gebruik van gezichtsherkenning of soortgelijke technologieën om emoties van een natuurlijke persoon af te leiden en 4) de verwerking van persoonsgegevens in een rechtshandhavingscontext die zou berusten op een database die massaal en op willekeurige wijze persoonsgegevens verzamelt, bijvoorbeeld door het “scrapen” van online toegankelijke foto’s en gezichtsopnamen.

Een centrale waarborg voor de grondrechten in kwestie is **doeltreffend toezicht** door de bevoegde toezichthoudende gegevensbeschermingsautoriteiten. Daarom moeten de lidstaten ervoor zorgen dat de middelen van de toezichthoudende autoriteiten passend en toereikend zijn om hen in staat te stellen hun mandaat te vervullen.

Deze **richtsnoeren zijn gericht op** beleidsmakers op EU- en nationaal niveau, alsmede op rechtshandhavingsinstanties en hun functionarissen die systemen voor gezichtsherkenningstechnologie implementeren en gebruiken. Personen komen aan bod voor zover zij in het algemeen of als betrokkenen een belang hebben, met name als het gaat om de rechten van betrokkenen.

De **richtsnoeren zijn bedoeld** om informatie te verstrekken over bepaalde eigenschappen van gezichtsherkenningstechnologie en over het toepasselijke rechtskader in de context van rechtshandhaving (in het bijzonder de RGR).

- Daarnaast bieden ze een **instrument voor een eerste indeling van de gevoeligheid van een gegeven gebruikssituatie** (bijlage I).
- Ze bevatten ook **praktische adviezen voor rechtshandhavingsinstanties die een gezichtsherkenningstechnologiesysteem willen aanschaffen en beheren** (bijlage II).

- In de richtsnoeren worden ook verschillende kenmerkende **gebruikssituaties beschreven en talrijke relevante overwegingen vermeld**, vooral met betrekking tot de noodzakelijkheids- en evenredigheidstoets (bijlage III).

1 INLEIDING

1. Gezichtsherkenningstechnologie kan worden gebruikt om personen automatisch te herkennen op basis van hun gezicht. Deze technologie is vaak gebaseerd op artificiële intelligentie, zoals technologieën voor machinaal leren. Toepassingen van gezichtsherkenningstechnologie worden steeds vaker op verschillende gebieden getest en gebruikt, van persoonlijk gebruik tot gebruik door particuliere organisaties en overheidsdiensten. Rechtshandhavingsinstanties verwachten ook voordelen van het gebruik van gezichtsherkenningstechnologie. De technologie belooft oplossingen voor relatief nieuwe uitdagingen, zoals onderzoeken met een grote hoeveelheid vastgelegd bewijsmateriaal, maar ook voor bekende problemen, in het bijzonder met betrekking tot de onderbezetting voor observatie- en opsporingstaken.

2. De toegenomen interesse in gezichtsherkenningstechnologie is voor een belangrijk deel gebaseerd op de efficiëntie en schaalbaarheid van deze technologie. Tegelijkertijd brengen deze efficiëntie en schaalbaarheid nadelen met zich mee die inherent zijn aan de technologie en de toepassing ervan, ook op grote schaal. Terwijl met één druk op een knop duizenden reeksen persoonsgegevens kunnen worden geanalyseerd, kunnen zelfs geringe gevolgen van algoritmische discriminatie of verkeerde identificatie ernstig invloed hebben op het gedrag en dagelijks leven van grote aantallen mensen. Alleen al de omvang van de verwerking van persoonsgegevens, en in het bijzonder van biometrische gegevens, is een ander belangrijk element van gezichtsherkenningstechnologie, aangezien het verwerken van persoonsgegevens een inmenging vormt in het grondrecht op de bescherming van persoonsgegevens overeenkomstig artikel 8 van het Handvest van de grondrechten van de Europese Unie (het Handvest).

3. De toepassing van gezichtsherkenningstechnologie door rechtshandhavingsinstanties zal aanzienlijke gevolgen hebben – en heeft deze tot op zekere hoogte al – voor individuen en groepen mensen, waaronder minderheden. Deze gevolgen zullen ook in belangrijke mate van invloed zijn op onze manier van samenleven en op onze sociale en democratische politieke stabiliteit, waarin waarde wordt gehecht aan de grote betekenis van pluralisme en politieke oppositie. Het recht op de bescherming van persoonsgegevens is vaak van essentieel belang als voorwaarde voor het waarborgen van andere grondrechten. De toepassing van gezichtsherkenningstechnologie is in aanzienlijke mate gevoelig voor inmenging in de grondrechten die buiten het recht op bescherming van persoonsgegevens liggen.

4. De EDPB acht het daarom belangrijk een bijdrage te leveren aan de voortdurende integratie van gezichtsherkenningstechnologie op het gebied van rechtshandhaving dat valt onder de richtlijn gegevensbescherming bij rechtshandhaving[1], respectievelijk de nationale wetten waarin deze richtlijn is omgezet, en de onderhavige richtsnoeren te verstrekken. De richtsnoeren zijn bedoeld om relevante informatie te verstrekken aan wetgevers op EU- en nationaal niveau, alsook aan rechtshandhavingsinstanties en hun functionarissen bij de invoering en het gebruik van gezichtsherkenningssystemen. Het toepassingsgebied van de richtsnoeren is beperkt tot

[1] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

gezichtsherkenningstechnologie. Andere vormen van verwerking van persoonsgegevens door rechtshandhavingsinstanties op basis van biometrische gegevens, met name als deze op afstand worden verwerkt, kunnen echter vergelijkbare of bijkomende risico's voor personen, groepen en de samenleving met zich meebrengen. Afhankelijk van de respectieve omstandigheden kunnen sommige aspecten van deze richtsnoeren ook in deze gevallen als een nuttige bron dienen. Ten slotte kunnen de richtsnoeren ook belangrijke informatie bevatten voor personen die in het algemeen of als betrokkenen een belang hebben, in het bijzonder met betrekking tot de rechten van betrokkenen.

5. De richtsnoeren bestaan uit het hoofddocument en drie bijlagen. In het onderhavige hoofddocument worden de technologie en het toepasselijke rechtskader gepresenteerd. Bijlage I bevat een sjabloon om enkele van de belangrijkste aspecten voor het classificeren van de ernst van de inmenging in de grondrechten voor een bepaald toepassingsgebied in kaart te brengen. Rechtshandhavingsinstanties die een gezichtsherkenningssysteem willen aanschaffen en gebruiken, kunnen praktische adviezen vinden in bijlage II. Afhankelijk van het toepassingsgebied van de gezichtsherkenningstechnologie kunnen verschillende overwegingen van belang zijn. Een reeks hypothetische scenario's en relevante overwegingen is te vinden in bijlage III.

2 TECHNOLOGIE

2.1 Eén biometrische technologie, twee verschillende functies

6. Gezichtsherkenning is een op kansberekening gebaseerde technologie die personen automatisch op basis van hun gezicht kan herkennen om hen te authenticeren of te identificeren.

7. De gezichtsherkenningstechnologie valt binnen de bredere categorie van biometrische technologie. Biometrie omvat alle geautomatiseerde processen die worden gebruikt om een individu te herkennen aan de hand van het kwantificeren van fysieke, fysiologische of gedragskenmerken (vingerafdrukken, irisstructuur, stem, manier van lopen, bloedvatpatronen enz.). Deze kenmerken worden gedefinieerd als "biometrische gegevens" omdat zij de unieke identificatie van die persoon mogelijk maken of bevestigen.

8. Dit is het geval bij de gezichten van mensen of, meer specifiek, de technische verwerking ervan met behulp van gezichtsherkenningsapparatuur: aan de hand van de afbeelding van een gezicht (een foto of video), een zogenoemd biometrisch "monster", is het mogelijk om een digitale weergave van de onderscheidende kenmerken van dit gezicht te extraheren (dit wordt een "template" genoemd).

9. Een biometrische template is een digitale weergave van de unieke kenmerken die uit een biometrisch monster zijn verkregen en kan in een biometrische database worden opgeslagen[2]. Deze template wordt verondersteld voor elke persoon uniek en specifiek te zijn en blijft in beginsel constant in de loop der tijd[3]. In de herkenningsfase vergelijkt het apparaat deze template met andere templates die eerder zijn geproduceerd of direct zijn berekend op basis van biometrische monsters, zoals gezichten op een afbeelding, foto of video. "Gezichtsherkenning" is derhalve een proces in twee stappen: het verzamelen van de gezichtsopname en het omzetten ervan in een template, gevolgd door de herkenning van dit gezicht door de betreffende template met een of meer andere templates te vergelijken.

[2] Richtsnoeren inzake gezichtsherkenning, Raadgevend Comité van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108), Raad van Europa, juni 2021.

[3] Dit kan afhangen van het soort biometrie en de leeftijd van de betrokkene.

10. Zoals elk biometrisch proces kan gezichtsherkenning twee verschillende functies vervullen:

    - de **authenticatie** van een persoon, bedoeld om na te gaan of iemand is wie hij of zij beweert te zijn. In dit geval vergelijkt het systeem een vooraf geregistreerde biometrische template of een monster (dat bijvoorbeeld is opgeslagen op een smartcard of in een biometrisch paspoort) met een enkel gezicht, bijvoorbeeld van een persoon die bij een controlepost verschijnt, om te verifiëren of het om een en dezelfde persoon gaat. Deze functionaliteit is derhalve gestoeld op de vergelijking van twee templates. Dit wordt ook wel één-op-één**verificatie** genoemd;

    - de **identificatie** van een persoon, gericht op het vinden van iemand in een groep personen, binnen een specifiek gebied, op een afbeelding of in een database. In dit geval moet het systeem elk vastgelegd gezicht verwerken om een biometrische template te genereren, en vervolgens controleren of deze overeenkomt met een persoon die bekend is in het systeem. Deze functionaliteit berust dus op het vergelijken van één template met een database van templates of monsters (het referentiepunt). Dit wordt ook wel één-op-velenidentificatie genoemd. Hierbij kan bijvoorbeeld een registratie van een persoonsnaam (achternaam, voornaam) aan een gezicht worden gekoppeld als de registratie wordt vergeleken met een database van foto's waaraan voor- en achternamen zijn gekoppeld. Het kan ook gaan om het volgen van een persoon in een menigte, zonder dat er noodzakelijkerwijs een verband wordt gelegd met de burgerlijke identiteit van de persoon.

11. In beide gevallen zijn de gebruikte gezichtsherkenningstechnieken gebaseerd op een geschatte overeenstemming (match) tussen templates: de template die wordt vergeleken en het/de referentiepunt(en). In dit opzicht zijn de technieken probabilistisch: uit de vergelijking wordt met een hogere of lagere graad van waarschijnlijkheid afgeleid dat de persoon inderdaad de persoon is die moet worden geauthenticeerd of geïdentificeerd; als deze waarschijnlijkheid boven een bepaalde door de gebruiker of de ontwikkelaar van het systeem gedefinieerde drempel in het systeem komt, zal het systeem aannemen dat er een match is.

12. Hoewel beide functies – authenticatie en identificatie – verschillend zijn, hebben zij beide betrekking op de verwerking van biometrische gegevens van een geïdentificeerde of identificeerbare natuurlijke persoon en vormen derhalve een verwerking van persoonsgegevens en meer in het bijzonder een verwerking van bijzondere categorieën persoonsgegevens.

13. Gezichtsherkenning maakt deel uit van een breder spectrum van technieken voor de verwerking van videobeelden. Sommige videocamera's kunnen mensen binnen een bepaald gebied filmen, met name hun gezichten, maar kunnen niet als zodanig worden gebruikt om personen automatisch te herkennen. Hetzelfde geldt voor eenvoudige fotografie: een camera is geen gezichtsherkenningssysteem omdat foto's van mensen op een specifieke manier moeten worden verwerkt om er biometrische gegevens uit te kunnen extraheren.

14. De loutere detectie van gezichten door zogenaamde "slimme" camera's vormt evenmin noodzakelijkerwijs een gezichtsherkenningssysteem. Hoewel ze ook belangrijke vragen opwerpen op het gebied van ethiek en doeltreffendheid, kunnen digitale technieken voor het opsporen van abnormaal gedrag of gewelddadige gebeurtenissen, of voor het herkennen van gezichtsemoties of zelfs silhouetten, niet worden beschouwd als biometrische systemen waarin bijzondere categorieën persoonsgegevens worden verwerkt, mits ze niet tot doel hebben een persoon op unieke wijze te identificeren en de betrokken verwerking van persoonsgegevens geen andere bijzondere categorieën van persoonsgegevens omvat. Deze voorbeelden staan niet volledig los van gezichtsherkenning en zijn

nog steeds onderworpen aan de regels inzake de bescherming van persoonsgegevens[4]. Bovendien kunnen dit soort detectiesystemen worden gebruikt in combinatie met andere systemen voor het identificeren van een persoon en derhalve worden beschouwd als gezichtsherkenningstechnologie.

15. In tegenstelling tot bijvoorbeeld systemen voor het opnemen en verwerken van video, waarvoor de installatie van fysieke apparaten vereist is, is gezichtsherkenning een softwarefunctionaliteit die kan worden uitgevoerd in bestaande systemen (camera's, beelddatabases enz.). Deze functionaliteit kan dus worden verbonden of gekoppeld met een veelvoud aan systemen of worden gecombineerd met andere functionaliteiten. Aan een dergelijke integratie in een al bestaande infrastructuur moet specifiek aandacht worden besteed, omdat dit onlosmakelijk risico's met zich meebrengt vanwege het feit dat de gezichtsherkenningstechnologie gemakkelijk te gebruiken kan zijn en gemakkelijk verborgen kan worden[5].

2.2 Een grote verscheidenheid aan doeleinden en toepassingen

16. Buiten het toepassingsgebied van deze richtsnoeren en buiten het toepassingsgebied van de RGR kan gezichtsherkenning worden gebruikt voor een breed scala aan doelstellingen, zowel voor commercieel gebruik als voor het aanpakken van problemen op het gebied van openbare veiligheid of rechtshandhaving. De technologie kan in veel verschillende contexten worden toegepast: in de persoonlijke relatie tussen een gebruiker en een dienst (toegang tot een applicatie), voor toegang tot een specifieke plaats (fysieke filtering) of zonder enige bijzondere beperking in de openbare ruimte (live gezichtsherkenning). Gezichtsherkenning kan worden ingezet voor elk soort betrokkene: een klant van een dienst, een werknemer, een eenvoudige toeschouwer, een gezocht persoon of iemand die betrokken is bij een gerechtelijke of administratieve procedure enz. Sommige toepassingen zijn al gemeengoed en wijdverbreid; andere bevinden zich op dit moment in een experimentele of speculatieve fase. Hoewel in deze richtsnoeren niet alle vormen van gebruik en toepassing worden behandeld, herinnert de EDPB eraan dat deze alleen mogen worden geïmplementeerd als ze in overeenstemming zijn met het toepasselijke wettelijke kader, in het bijzonder met de AVG en relevante nationale wetgeving.[6] Ook in het kader van de RGR kunnen, naast de functies van authenticatie of identificatie, gegevens die met behulp van gezichtsherkenningstechnologie zijn verwerkt, ook voor andere doeleinden verder worden verwerkt, bijvoorbeeld om ze in te delen.

17. Meer in het bijzonder kan een schaal van mogelijke toepassingen worden overwogen, afhankelijk van de mate waarin personen zeggenschap hebben over hun persoonsgegevens, de effectieve middelen die ze hebben om deze zeggenschap uit te oefenen en hun recht op initiatief om deze technologie in werking te stellen en te gebruiken, de gevolgen voor hen (bij herkenning of niet-herkenning) en de schaal van de uitgevoerde verwerking. Gezichtsherkenning op basis van een template die is opgeslagen op een persoonlijk apparaat (smartcard, smartphone enz.) van de betreffende persoon, waarmee die persoon zich identificeert en dat uitsluitend is bedoeld voor persoonlijk gebruik via een speciale interface, brengt niet dezelfde risico's met zich mee als bijvoorbeeld het gebruik van gezichtsherkenning voor identificatiedoeleinden in een ongecontroleerde omgeving, zonder actieve inmenging van de betrokkenen, waarbij de template van elke persoon die het bewaakte gebied betreedt, wordt vergeleken met de templates van een brede dwarsdoorsnede van de bevolking die in

[4] Artikel 10 RGR (of artikel 9 AVG) is echter wel van toepassing op systemen die worden gebruikt om personen op basis van hun biometrische gegevens in te delen in clusters op grond van etnische afkomst, politieke overtuiging, seksuele gerichtheid of andere bijzondere categorieën persoonsgegevens.
[5] Bijvoorbeeld in de bodycams die in de praktijk steeds vaker worden gebruikt.
[6] Zie voor meer informatie ook de richtsnoeren 3/2019 van de EDPB inzake de verwerking van persoonsgegevens door middel van videoapparatuur, zoals vastgesteld op 29 januari 2020.

een database zijn opgeslagen. Tussen deze twee uitersten ligt een zeer gevarieerd spectrum van toepassingen en bijbehorende problemen met betrekking tot de bescherming van persoonsgegevens.

18. Voor een nadere illustratie van de context waarin gezichtsherkenningstechnologieën momenteel worden besproken of ingevoerd, hetzij voor authenticatie of identificatie, acht de EDPB het relevant om een reeks voorbeelden te noemen. De onderstaande voorbeelden zijn louter beschrijvend en mogen niet worden beschouwd als een voorlopige beoordeling van hun naleving van het EU-acquis op het gebied van gegevensbescherming.

Voorbeelden van gezichtsherkenning voor authenticatie

19. Authenticatie kan zodanig worden ontworpen dat gebruikers er volledige zeggenschap over hebben, bijvoorbeeld om louter in een thuisomgeving de toegang tot diensten of toepassingen in te schakelen. Als zodanig wordt het op grote schaal door smartphonebezitters gebruikt om hun apparaat te ontgrendelen in plaats van authenticatie via een wachtwoord.

20. Authenticatie met gezichtsherkenning kan ook worden gebruikt om de identiteit te controleren van iemand die gebruik wenst te maken van openbare of particuliere diensten van derden. Dergelijke processen bieden dus een manier om met behulp van een mobiele app (smartphone, tablet enz.) een digitale identiteit te creëren die vervolgens kan worden gebruikt om toegang te krijgen tot online administratieve diensten.

21. Verder kan gezichtsherkenningsauthenticatie tot doel hebben de fysieke toegang tot een of meer vooraf bepaalde locaties te controleren, zoals ingangen van gebouwen of specifieke doorlaatposten. Deze functionaliteit wordt bijvoorbeeld toegepast in bepaalde verwerkingen bij grensovergangen, waarbij het gezicht van de persoon op het apparaat wordt vergeleken met het gezicht dat in het identiteitsbewijs (paspoort of vaste verblijfsvergunning) is opgeslagen.

Voorbeelden van gezichtsherkenning voor identificatie

22. Identificatie kan op vele, nog meer uiteenlopende manieren worden toegepast. Voorbeelden hiervan zijn de hieronder vermelde toepassingen die momenteel in de EU worden waargenomen, getest of gepland:

- in een database met foto's zoeken naar de identiteit van een niet-geïdentificeerde persoon (slachtoffer, verdachte enz.);
- de bewegingen van een persoon in de openbare ruimte volgen. Het gezicht van die persoon wordt vergeleken met de biometrische templates van personen die in het bewaakte gebied reizen of hebben gereisd, bijvoorbeeld wanneer een stuk bagage is achtergelaten of nadat een strafbaar feit is gepleegd;
- reconstructie van de reis van een persoon en de daaropvolgende interacties met andere personen, door middel van een latere vergelijking van dezelfde elementen in een poging om bijvoorbeeld hun contacten te identificeren;
- biometrische identificatie op afstand van gezochte personen in openbare ruimten. Alle gezichten die live worden vastgelegd door videobewakingscamera's worden in real time vergeleken met een database van de veiligheidsdiensten;
- automatische herkenning van mensen in een afbeelding, bijvoorbeeld om hun relaties te identificeren op een sociaal netwerk dat dit gebruikt. De afbeelding wordt vergeleken met de

templates van iedereen op het netwerk die met deze functionaliteit heeft ingestemd teneinde de geïdentificeerde namen van deze relaties voor te stellen;

- toegang tot diensten, waarbij sommige geldautomaten hun klanten herkennen door een met een camera opgenomen gezicht te vergelijken met de database van gezichtsopnamen van de bank;

- de reis van een passagier volgen in een bepaalde fase van de reis. De in real time berekende template van iemand die incheckt bij poortjes in bepaalde fasen van de reis (bagageafgiftepunten, instappoortjes enz.), wordt vergeleken met de templates van personen die eerder in het systeem zijn geregistreerd.

23. Het gebruik van gezichtsherkenningstechnologie op het gebied van rechtshandhaving met daarnaast het brede scala aan waargenomen toepassingen vraagt zonder meer om een uitgebreid debat en een omvattende beleidsaanpak om de consistentie en naleving van het EU-acquis op het gebied van gegevensbescherming te waarborgen.

2.3 Betrouwbaarheid, nauwkeurigheid en risico's voor betrokkenen

24. Zoals bij elke technologie kunnen ook bij de uitvoering van gezichtsherkenning uitdagingen optreden, in het bijzonder als het gaat om de betrouwbaarheid en doeltreffendheid in termen van authenticatie of identificatie, evenals de algemene kwestie van kwaliteit en nauwkeurigheid van de "bron"-gegevens en het resultaat van de verwerking van gezichtsherkenningstechnologie.

25. Dergelijke technologische uitdagingen brengen bijzondere risico's voor de betrokkenen met zich mee, die gezien de mogelijke juridische of andere gevolgen die de betrokkenen op soortgelijke wijze in aanzienlijke mate treffen, des te groter of ernstiger zijn op het gebied van rechtshandhaving. In dit kader lijkt het ook nuttig om te benadrukken dat het achteraf gebruiken van gezichtsherkenningstechnologie niet per se veiliger is, aangezien individuen in tijd en plaats kunnen worden gevolgd. Het gebruik achteraf brengt dus ook specifieke risico's met zich mee, die per geval moeten worden beoordeeld.[7]

26. Het Bureau van de Europese Unie voor de grondrechten merkt in zijn verslag van 2019 op dat het bepalen van het noodzakelijke nauwkeurigheidsniveau van gezichtsherkenningssoftware een uitdaging is en dat er veel verschillende manieren zijn om de nauwkeurigheid te beoordelen en te evalueren, ook afhankelijk van de taak, het doel en de context van het gebruik ervan. Bij het toepassen van de technologie op plaatsen die door miljoenen mensen worden bezocht, zoals treinstations of luchthavens, betekent een relatief klein percentage fouten (bijv. 0,01 %)[8] dat er toch nog honderden mensen ten onrechte worden gemarkeerd. Bovendien is het mogelijk dat bij bepaalde categorieën personen de kans op een onjuiste match groter is dan bij anderen, zoals beschreven in hoofdstuk 3. Foutenpercentages kunnen op verschillende manieren worden berekend en geïnterpreteerd, dus voorzichtigheid is geboden. Daarnaast zijn, als het gaat om nauwkeurigheid en fouten, vragen met betrekking tot hoe gemakkelijk een systeem kan worden misleid door bijvoorbeeld valse gezichtsfoto's ("spoofing" genoemd) belangrijk, met name voor rechtshandhavingsdoeleinden.[9]

27. In dit verband vindt de EDPB het belangrijk eraan te herinneren dat gezichtsherkenningstechnologie, ongeacht of deze voor authenticatie of voor identificatie wordt gebruikt, geen doorslaggevend

[7] Zie de voorbeelden in bijlage III.

[8] Dit nauwkeurigheidspercentage komt uit het aangehaalde rapport en weerspiegelt een percentage dat veel beter is dan de huidige prestaties van algoritmen in toepassingen van gezichtsherkenningstechnologie.

[9] "Facial recognition technology: fundamental rights considerations in the context of law enforcement" (Gezichtsherkenningstechnologie: overwegingen op het gebied van de grondrechten in het kader van rechtshandhaving), Bureau van de Europese Unie voor de grondrechten, 21 november 2019.

resultaat oplevert, maar gebaseerd is op de waarschijnlijkheid dat twee gezichten, of afbeeldingen van gezichten, overeenstemmen met dezelfde persoon.[10] Dit resultaat wordt nog slechter wanneer de kwaliteit van de ingevoerde biometrische monsters voor de gezichtsherkenning laag is. Invoer van onscherpe beelden, een lage resolutie van de camera, beweging en slechte verlichting kunnen factoren voor een lage kwaliteit zijn. Andere aspecten die een significante invloed hebben op de resultaten zijn prevalentie en spoofing, bijvoorbeeld wanneer criminelen proberen te voorkomen dat ze langs de camera's lopen of proberen de gezichtsherkenningstechnologie te misleiden. Talrijke studies hebben ook aangetoond dat dergelijke statistische resultaten van algoritmische verwerking onderhevig kunnen zijn aan vooringenomenheid, met name als gevolg van de kwaliteit van de brongegevens en de trainingsdatabases of door andere factoren, zoals de keuze van de locatie waar de technologie wordt ingezet. Voorts moet ook worden gewezen op de gevolgen van gezichtsherkenningstechnologie voor andere grondrechten, zoals de eerbiediging van het privéleven en het familie- en gezinsleven, de vrijheid van meningsuiting en van informatie, de vrijheid van vergadering en vereniging enz.

28. Het is daarom van essentieel belang dat de betrouwbaarheid en nauwkeurigheid van gezichtsherkenningstechnologie in aanmerking worden genomen als criteria bij de beoordeling van de naleving van de belangrijkste gegevensbeschermingsbeginselen, overeenkomstig artikel 4 RGR. Dit geldt met name wanneer het gaat om billijkheid en nauwkeurigheid.

29. De EDPB benadrukt dat gegevens van hoge kwaliteit essentieel zijn voor algoritmen van hoge kwaliteit, maar benadrukt tegelijkertijd dat verwerkingsverantwoordelijken, als onderdeel van hun verantwoordingsplicht, de algoritmische verwerking regelmatig en systematisch moeten evalueren om met name de nauwkeurigheid, billijkheid en betrouwbaarheid van het resultaat van deze verwerking van persoonsgegevens te waarborgen. Persoonsgegevens die worden gebruikt met het oog op het evalueren, trainen en verder ontwikkelen van systemen voor gezichtsherkenningstechnologie, mogen alleen worden verwerkt op basis van een toereikende rechtsgrondslag en in overeenstemming met de gangbare beginselen voor gegevensbescherming.

3 TOEPASSELIJK RECHTSKADER

30. Het gebruik van gezichtsherkenningstechnologieën is onlosmakelijk verbonden met de verwerking van persoonsgegevens, met inbegrip van bijzondere categorieën gegevens. Bovendien heeft het direct of indirect gevolgen voor een aantal grondrechten die zijn vastgelegd in het Handvest van de grondrechten van de EU. Dit is met name van belang op het gebied van rechtshandhaving en strafrecht. Daarom moet elk gebruik van gezichtsherkenningstechnologieën worden uitgevoerd in strikte overeenstemming met het toepasselijke wettelijke kader.

31. De volgende informatie is bedoeld om in overweging te worden genomen bij de beoordeling van toekomstige wettelijke en bestuursrechtelijke maatregelen en bij de uitvoering van bestaande wetgeving in elk geval waarin gezichtsherkenningstechnologie wordt gebruikt. De relevantie van de respectieve vereisten varieert naargelang de specifieke omstandigheden. Aangezien niet alle toekomstige omstandigheden kunnen worden voorzien, wordt de informatie slechts beschouwd als ondersteunend en mag deze niet worden uitgelegd als een uitputtende opsomming.

[10] Deze waarschijnlijkheid wordt de "betrouwbaarheidsscore" genoemd.

3.1 Algemeen rechtskader – Het Handvest van de grondrechten van de EU en het Europees Verdrag voor de rechten van de mens (EVRM)

3.1.1 Toepasselijkheid van het Handvest

32. Het Handvest van de grondrechten van de Europese Unie (hierna "het Handvest") is gericht tot de instellingen, organen en instanties van de Unie en tot de lidstaten wanneer zij het recht van de Unie ten uitvoer brengen.

33. De regulering van de verwerking van biometrische gegevens voor rechtshandhavingsdoeleinden overeenkomstig artikel 1, lid 1, RGR, doet onvermijdelijk de vraag rijzen naar de naleving van de grondrechten, in het bijzonder de eerbiediging van het privéleven en van communicatie uit hoofde van artikel 7 van het Handvest en het recht op bescherming van persoonsgegevens uit hoofde van artikel 8 van het Handvest.

34. Het verzamelen en analyseren van videobeelden van natuurlijke personen, waaronder hun gezichten, houdt de verwerking van persoonsgegevens in. Bij een technische verwerking van het beeld omvat de verwerking ook biometrische gegevens. De technische verwerking van gegevens die betrekking hebben op het gezicht van een natuurlijke persoon in relatie tot tijd en plaats maakt het mogelijk om conclusies te trekken over het privéleven van de betrokken personen. Deze conclusies kunnen betrekking hebben op de raciale of etnische afkomst, gezondheid, religie, dagelijkse leefgewoonten, permanente of tijdelijke verblijfplaatsen, dagelijkse of andere verplaatsingen, uitgevoerde activiteiten of sociale relaties van deze personen en de sociale omgevingen die door hen worden bezocht. Uit de grote verscheidenheid aan informatie die de toepassing van gezichtsherkenningstechnologie kan opleveren, blijkt duidelijk wat de mogelijke gevolgen zijn voor het in artikel 8 van het Handvest vastgelegde recht op de bescherming van persoonsgegevens, maar ook op het in artikel 7 van het Handvest vastgelegde recht op eerbiediging van het privéleven.

35. In dergelijke omstandigheden is het ook niet ondenkbaar dat het verzamelen, analyseren en verder verwerken van de betrokken biometrische (gezichts-)gegevens gevolgen kan hebben voor de manier waarop mensen zich vrij voelen om te handelen, zelfs als de handeling volledig binnen de grenzen van een vrije en open samenleving valt. Het kan ook ernstige gevolgen hebben voor de uitoefening van hun grondrechten, zoals het recht op vrijheid van gedachte, geweten en godsdienst, op vrijheid van meningsuiting en op vreedzame vergadering en vrijheid van vereniging overeenkomstig de artikelen 1, 10, 11 en 12 van het Handvest. Een dergelijke verwerking brengt ook andere risico's met zich mee, zoals het risico op misbruik van de door de bevoegde autoriteiten verzamelde persoonsgegevens als gevolg van de onrechtmatige toegang tot en het onrechtmatige gebruik van de persoonsgegevens, inbreuken op de beveiliging enz. De risico's hangen vaak af van de verwerking en de omstandigheden waaronder deze plaatsvindt, zoals het risico op onrechtmatige toegang en onrechtmatig gebruik door politiefunctionarissen of andere onbevoegde partijen. Sommige risico's zijn echter simpelweg inherent aan het unieke karakter van biometrische gegevens. In tegenstelling tot een adres of een telefoonnummer is het voor een betrokkene onmogelijk om zijn of haar unieke kenmerken, zoals het gezicht of de iris, te wijzigen. In het geval van ongeoorloofde toegang of onopzettelijke bekendmaking van biometrische gegevens zou dit ertoe leiden dat het gebruik van de gegevens als wachtwoord of cryptografische sleutel wordt gecompromitteerd of dat de gegevens kunnen worden gebruikt voor nadere, niet-geautoriseerde observatieactiviteiten ten nadele van de betrokkene.

3.1.2 Inmenging in de in het Handvest neergelegde rechten

36. Het onder alle omstandigheden verwerken van biometrische gegevens vormt een ernstige inmenging op zich. Dit staat los van de uitkomst, zoals een positieve match. De verwerking vormt een inmenging,

zelfs als de biometrische template onmiddellijk wordt gewist nadat de vergelijking met een politiedatabase geen match heeft opgeleverd.

37. De inmenging in de grondrechten van de betrokkenen kan voortvloeien uit een rechtshandeling die tot doel of tot gevolg heeft dat het desbetreffende grondrecht wordt beperkt[11]. Zij kan ook het resultaat zijn van een handeling van een overheidsinstantie met hetzelfde doel of dezelfde strekking of zelfs van een privaatrechtelijke entiteit die bij wet is belast met de uitoefening van het openbaar gezag en de openbare bevoegdheden.

38. Een wetgevende maatregel die als rechtsgrond dient voor de verwerking van persoonsgegevens, grijpt rechtstreeks in in de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten[12].

39. Het gebruik van biometrische gegevens en gezichtsherkenningstechnologie in het bijzonder heeft in veel gevallen ook gevolgen voor het recht op de menselijke waardigheid, dat wordt gewaarborgd door artikel 1 van het Handvest. Menselijke waardigheid vereist dat personen niet als louter objecten worden behandeld. Gezichtsherkenningstechnologie rekent existentiële en zeer persoonlijke kenmerken, de gelaatstrekken, om naar een machineleesbare vorm met als doel deze te gebruiken als een menselijke nummerplaat of ID-kaart, waardoor het gezicht geobjectiveerd wordt.

40. Een dergelijke verwerking kan ook ingrijpen in andere grondrechten, zoals de rechten uit hoofde van de artikelen 10, 11 en 12 van het Handvest, voor zover de betreffende videobewaking van de rechtshandhavingsinstanties is bedoeld om angst op te wekken of hieruit gevoelens van angst voortvloeien.

41. Daarnaast moet ook zorgvuldig worden gekeken naar de potentiële risico's van het gebruik van gezichtsherkenningstechnologieën door rechtshandhavers met betrekking tot het recht op een eerlijk proces en het vermoeden van onschuld op grond van de artikelen 47 en 48 van het Handvest. Het resultaat van de toepassing van gezichtsherkenningstechnologie, zoals een match, kan er niet alleen toe leiden dat een persoon aan verder politieoptreden wordt onderworpen, maar kan ook doorslaggevend bewijs zijn in gerechtelijke procedures. Tekortkomingen van de gezichtsherkenningstechnologie zoals mogelijke vooringenomenheid, discriminatie of verkeerde identificatie ("foutpositieven") kunnen dus ook ernstige gevolgen hebben voor strafprocedures. Bovendien kan bij de beoordeling van het bewijs de voorkeur worden gegeven aan het resultaat van de toepassing van de gezichtsherkenningstechnologie, ook als er sprake is van tegenstrijdig bewijs (de zogenaamde "automation bias").

3.1.3 Rechtvaardiging voor de inmenging

42. Overeenkomstig artikel 52, lid 1, van het Handvest moeten beperkingen op de uitoefening van grondrechten en vrijheden bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. Met inachtneming van het evenredigheidsbeginsel kunnen er alleen beperkingen worden gesteld indien deze noodzakelijk zijn en daadwerkelijk voldoen aan door de Europese Unie erkende doelstellingen van algemeen belang of aan de noodzaak de rechten en vrijheden van anderen te beschermen.

3.1.3.1 Bij wet gesteld

43. In artikel 52, lid 1, van het Handvest is het vereiste van een specifieke rechtsgrondslag vastgelegd. De formulering van deze rechtsgrondslag moet voldoende duidelijk zijn om de burgers een adequate

[11] HvJ-EU, C-219/91, Ter Voort, Jurispr. 1992, blz. I-05485, punt 37; HvJ-EU, C-200/96, Metronome, Jurispr. 1998, blz. I-1953, punt 28.
[12] HvJ-EU, C-594/12, punt 36; HvJ-EU, C-291/12, punten 23 e.v.

indicatie te geven van de voorwaarden waaronder en de omstandigheden waarin overheidsdiensten bevoegd zijn om gebruik te maken van maatregelen op het gebied van gegevensverzameling en geheime observatie[13]. Hierin moeten met redelijke duidelijkheid de reikwijdte en de wijze van uitoefening van de desbetreffende discretionaire bevoegdheid van de overheidsinstanties zijn aangegeven, teneinde individuen de minimale mate van bescherming te garanderen waarop zij uit hoofde van de rechtsstatelijkheid in een democratische samenleving recht hebben[14]. Bovendien vereist rechtmatigheid adequate waarborgen om ervoor te zorgen dat met name het recht van een persoon uit hoofde van artikel 8 van het Handvest wordt geëerbiedigd. Deze beginselen zijn ook van toepassing op de verwerking van persoonsgegevens met het oog op het evalueren, trainen en verder ontwikkelen van gezichtsherkenningstechnologiesystemen.

44. Aangezien biometrische gegevens die worden verwerkt met het oog op de unieke identificatie van een natuurlijke persoon vallen onder de bijzondere categorieën gegevens die worden vermeld in artikel 10 RGR zou voor de verschillende toepassingen van de gezichtsherkenningstechnologie in de meeste gevallen een specifieke wet vereist zijn waarin de toepassing en de voorwaarden voor het gebruik ervan nauwkeurig worden beschreven. Dit heeft met name betrekking op de soorten criminaliteit en, voor zover van toepassing, het gepaste ernstcriterium voor deze strafbare feiten, onder meer om kleine criminaliteit daadwerkelijk uit te sluiten[15].

3.1.3.2 De wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven en op de bescherming van persoonsgegevens, zoals vastgelegd in de artikelen 7 en 8 van het Handvest

45. Ook bij de beperkingen van de grondrechten die in elke situatie gelden, moet er in zijn voorzien dat de wezenlijke inhoud van het specifieke recht wordt geëerbiedigd. De wezenlijke inhoud heeft betrekking op de kern van het betrokken grondrecht[16]. Ook de menselijke waardigheid moet worden geëerbiedigd, zelfs wanneer een recht wordt beperkt[17].

46. Aanwijzingen voor een mogelijke inbreuk op de onaantastbare kern zijn de volgende:

- een bepaling die beperkingen oplegt ongeacht het individuele gedrag van een persoon of uitzonderlijke omstandigheden[18];
- een beroep op de rechter is niet mogelijk of wordt belemmerd[19];
- voorafgaand aan een ernstige beperking worden de omstandigheden van de betrokken persoon niet in aanmerking genomen[20];
- met het oog op de rechten uit hoofde van de artikelen 7 en 8 van het Handvest: naast het breed verzamelen van metagegevens over communicatie, kan ook de verwerving van de kennis van de inhoud van de elektronische communicatie een schending van de wezenlijke inhoud van die rechten vormen[21];
- met het oog op de rechten uit hoofde van de artikelen 7, 8 en 11 van het Handvest: wetgeving die aanbieders van toegang tot online openbare communicatiediensten en aanbieders van

[13] EHRM, Shimovolos tegen Rusland, § 68; Vukota-Bojić tegen Zwitserland.
[14] EHRM, Piechowicz tegen Polen, § 212.
[15] Zie bijv. de arresten van het HvJ-EU in de zaken C-817/19, Ligue des droits humains, punt 151, en C-207/16, Ministerio Fiscal, punt 56.
[16] HvJ-EU, C-279/09, Jurispr. 2010, blz. I-13849, punt 60.
[17] Toelichtingen bij het Handvest van de grondrechten, Titel I, Toelichting bij artikel 1, PB C 303 van 14.12.2007, blz. 17-35.
[18] HvJ-EU, C-601/15, punt 52.
[19] HvJ-EU, C-400/10, Jurispr. 2010, blz. I-08965, punt 55.
[20] HvJ-EU, C-408/03, Jurispr. 2006, blz. I-02647, punt 68.
[21] HvJ-EU – 203/15 – Tele2 Sverige, punt 101, onder verwijzing naar HvJ-EU – C-293/12 en C-594/12, punt 39.

hostingdiensten verplicht om in het algemeen en zonder onderscheid onder meer met deze diensten verband houdende persoonsgegevens te bewaren[22];

- onder verwijzing naar de rechten uit hoofde van artikel 8 van het Handvest: het ontbreken van de basisbeginselen voor gegevensbescherming en gegevensbeveiliging kan ook een inbreuk op de kern van het recht vormen[23].

3.1.3.3 Rechtmatig doel

47. Zoals reeds uiteengezet in punt 3.1.3., moeten de beperkingen op de grondrechten daadwerkelijk voldoen aan de door de Europese Unie erkende doelstellingen van algemeen belang of aan de noodzaak om de rechten en vrijheden van anderen te beschermen.

48. De Unie erkent zowel de doelstellingen die worden vermeld in artikel 3 van het Verdrag betreffende de Europese Unie als andere belangen die worden beschermd door specifieke bepalingen van de Verdragen[24], te weten onder andere een ruimte van vrijheid, veiligheid en recht en het voorkomen en bestrijden van strafbare feiten. In haar betrekkingen met de rest van de wereld moet de Unie bijdragen aan vrede en veiligheid en aan de bescherming van de mensenrechten.

49. De noodzaak om de rechten en vrijheden van anderen te beschermen heeft betrekking op de rechten van personen die beschermd worden door het recht van de Europese Unie of van haar lidstaten. De beoordeling moet worden uitgevoerd met het doel de vereisten van de bescherming van de respectieve rechten met elkaar in overeenstemming te brengen en een billijk evenwicht tussen deze rechten tot stand te brengen[25].

3.1.3.4 Noodzakelijkheids- en evenredigheidstoets

50. Wanneer er sprake is van inmenging in de grondrechten, kan de reikwijdte van de beoordelingsvrijheid van de nationale wetgever en de Uniewetgever beperkt blijken te zijn. Dit hangt af van een aantal factoren, waaronder het betrokken gebied, de aard van het betrokken recht dat door het Handvest wordt gegarandeerd, de aard en de ernst van de inmenging en het met de inmenging nagestreefde doel[26]. Wetgevingsmaatregelen moeten passend zijn voor het verwezenlijken van de legitieme doelstellingen die met de wetgeving in kwestie worden nagestreefd. Bovendien mag de maatregel niet de grenzen overschrijden van wat passend en noodzakelijk is om deze doelstellingen te bereiken[27]. Een doelstelling van algemeen belang, hoe wezenlijk zij ook is, rechtvaardigt op zich niet de beperking van een grondrecht[28].

51. Volgens vaste rechtspraak van het HvJ-EU mogen afwijkingen van en beperkingen op de bescherming van persoonsgegevens alleen worden toegepast voor zover dat strikt noodzakelijk is[29]. Dit houdt tevens

---

[22] HvJ-EU – C-512/18, La Quadrature du Net, punten 209 e.v.

[23] HvJ-EU – C-594/12, punt 40.

[24] Toelichtingen bij het Handvest van de grondrechten, Titel I, Toelichting bij artikel 52, PB C 303 van 14.12.2007, blz. 17-35.

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

[26] HvJ-EU – C-594/12, punt 47, met de volgende bronnen: zie, naar analogie voor wat betreft artikel 8 EVRM, EHRM, S. en Marper tegen het Verenigd Koninkrijk (Grote kamer), nrs. 30562/04 en 30566/04, § 102, ECHR 2008-V.

[27] HvJ-EU – C-594/12, punt 46 met de volgende bronnen: Zaak C-343/09, Afton Chemical, EU:C:2010:419, punt 45; Volker und Markus Schecke en Eifert, EU:C:2010:662, punt 74; zaken C-581/10 en C-629/10, Nelson e.a., EU:C:2012:657, punt 71; zaak C-283/11, Sky Österreich, EU:C:2013:28, punt 50, en zaak C-101/12, Schaible, EU:C:2013:661, punt 29.

[28] HvJ-EU – C-594/12, punt 51.

[29] HvJ-EU – C-594/12, punt 52, met de volgende bronnen: Zaak C-473/12, IPI EU:C:2013:715, punt 39 en aldaar aangehaalde rechtspraak.

in dat er geen minder ingrijpende middelen beschikbaar zijn om het doel te bereiken. Mogelijke alternatieven zoals extra personeel, frequenter politietoezicht of extra straatverlichting, afhankelijk van het beoogde doel, moeten zorgvuldig worden geïdentificeerd en beoordeeld. De wetgevingsmaatregelen moeten onderscheid maken tussen en gericht zijn op personen die in het licht van de doelstelling, bijvoorbeeld de bestrijding van ernstige strafbare feiten, onder de maatregel vallen. Als de maatregel algemeen van toepassing is op alle personen zonder dat er sprake is van een dergelijk onderscheid of een dergelijke beperking of uitzondering, wordt de inmenging versterkt[30]. De maatregel leidt tot een nog sterkere inmenging als de gegevensverwerking betrekking heeft op een aanzienlijk deel van de bevolking[31].

52. De bescherming van persoonsgegevens die voortvloeit uit de expliciete verplichting van artikel 8, lid 1, van het Handvest is met name belangrijk voor het recht op eerbiediging van het privéleven dat is vastgelegd in artikel 7 van het Handvest[32]. De wetgeving moet duidelijke en precieze regels vastleggen voor het toepassingsgebied en de toepassing van de maatregel in kwestie en waarborgen bieden zodat de personen van wie de gegevens zijn verwerkt, voldoende garanties hebben om hun persoonsgegevens doeltreffend te beschermen tegen het risico van misbruik en tegen elke onrechtmatige toegang tot of elk onrechtmatig gebruik van die gegevens[33]. De noodzaak voor dergelijke waarborgen is des te groter wanneer de persoonsgegevens automatisch worden verwerkt en wanneer er een aanzienlijk risico op onrechtmatige toegang tot de gegevens bestaat[34]. Daarnaast kan een interne of externe, bijvoorbeeld gerechtelijke, goedkeuring van de inzet van gezichtsherkenningstechnologie ook waarborgen bieden en noodzakelijk blijken in bepaalde gevallen van ernstige inmenging.[35]

53. De vastgestelde regels moeten worden aangepast aan de specifieke situatie, zoals de hoeveelheid verwerkte gegevens, de aard van de gegevens[36] en het risico op onrechtmatige toegang tot de gegevens. Dit vereist een regelgeving die met name ertoe zou dienen om de bescherming en beveiliging van de gegevens in kwestie op duidelijke en strikte wijze te regelen, teneinde de volledige integriteit en vertrouwelijkheid ervan te waarborgen[37].

54. Wat de relatie tussen de verwerkingsverantwoordelijke en de verwerker betreft, mag het niet zo zijn dat de verwerkers bij de bepaling van het op persoonsgegevens toegepaste beveiligingsniveau alleen rekening houden met economische overwegingen; dit zou een voldoende hoog beschermingsniveau in gevaar kunnen brengen[38].

55. In een rechtshandeling moeten materiële en procedurele voorwaarden en objectieve criteria worden vastgesteld op grond waarvan de grenzen van de toegang van de bevoegde autoriteiten tot gegevens en het latere gebruik ervan worden bepaald. Met het oog op het voorkomen, opsporen of vervolgen van strafbare feiten zouden de desbetreffende strafbare feiten als voldoende ernstig moeten worden

[30] HvJ-EU – C-594/12, punt 57.
[31] HvJ-EU – C-594/12, punt 56.
[32] HvJ-EU – C-594/12, punt 53.
[33] HvJ-EU – C-594/12, punt 54, met de volgende bronnen: zie, naar analogie voor wat betreft artikel 8 EVRM, EHRM, Liberty e.a. tegen het Verenigd Koninkrijk, 1 juli 2008, nr. 58243/00, §§ 62 en 63; Rotaru tegen Roemenië, §§ 57 tot en met 59, en S. en Marper tegen het Verenigd Koninkrijk, § 99.
[34] HvJ-EU – C-594/12, punt 55, met de volgende bronnen: zie, naar analogie voor wat betreft artikel 8 EVRM, S. en Marper tegen het Verenigd Koninkrijk, § 103 en M. K. tegen Frankrijk, 18 april 2013, nr. 19522/09, § 35.
[35] EHRM, Szabó en Vissy tegen Hongarije, §§ 73 t/m 77.
[36] Zie ook de strengere eisen voor technische en organisatorische maatregelen bij de verwerking van bijzondere categorieën gegevens, artikel 29, lid 1, RGR.
[37] HvJ-EU – C-594/12, punt 66.
[38] HvJ-EU – C-594/12, punt 67.

beschouwd om de omvang en de ernst van deze inmenging in de grondrechten zoals verankerd in bijvoorbeeld de artikelen 7 en 8 van het Handvest, te rechtvaardigen[39].

56. De gegevens moeten worden verwerkt op een wijze die de toepasselijkheid en het effect van de EU-regels inzake gegevensbescherming waarborgt, met name die van artikel 8 van het Handvest, waarin is bepaald dat de naleving van de eisen inzake bescherming en beveiliging onderworpen is aan toezicht door een onafhankelijke autoriteit. De geografische plaats waar de verwerking plaatsvindt, kan in een dergelijke situatie relevant zijn[40].

57. Bij de verschillende stappen in de verwerking van persoonsgegevens moeten de categorieën gegevens worden onderscheiden op basis van hun mogelijke bruikbaarheid voor de verwezenlijking van het nagestreefde doel of overeenkomstig de betrokken personen[41]. De vaststelling van de voorwaarden van de verwerking, bijvoorbeeld de bepaling van de bewaartermijn, moet gebaseerd zijn op objectieve criteria om te waarborgen dat de inmenging wordt beperkt tot wat strikt noodzakelijk is[42].

58. Op basis van elke situatie moeten bij de beoordeling van de noodzakelijkheid en evenredigheid alle implicaties worden vastgesteld en in aanmerking worden genomen die binnen het toepassingsgebied van andere grondrechten vallen, zoals de menselijke waardigheid uit hoofde van artikel 1 van het Handvest, de vrijheid van gedachte, geweten en godsdienst uit hoofde van artikel 10 van het Handvest, de vrijheid van meningsuiting uit hoofde van artikel 11 van het Handvest en de vrijheid van vergadering en vereniging uit hoofde van artikel 12 van het Handvest.

59. Bovendien moet het ook als een ernstige zaak worden beschouwd dat als de gegevens systematisch worden verwerkt zonder dat de betrokkenen hiervan op de hoogte zijn, dit waarschijnlijk een algemeen gevoel opwekt dat men constant in de gaten wordt gehouden[43]. Dit kan leiden tot gevoelens van angst met betrekking tot sommige of alle betrokken grondrechten.

60. Om de beoordeling van de noodzakelijkheid en evenredigheid in wetgevingsmaatregelen met betrekking tot gezichtsherkenning op het gebied van rechtshandhaving te vergemakkelijken en te operationaliseren, zouden de nationale en Uniewetgevers gebruik kunnen maken van de speciaal voor deze taak ontworpen praktische instrumenten die beschikbaar zijn. Met name kan gebruik worden gemaakt van de door de Europese Toezichthouder voor gegevensbescherming verstrekte toolkit[44] over noodzakelijkheid en evenredigheid.

3.1.3.5 Artikel 52, lid 3, en artikel 53 van het Handvest (beschermingsniveau, ook in relatie tot het beschermingsniveau van het EVRM)

61. Overeenkomstig artikel 52, lid 3, en artikel 53 van het Handvest moeten de inhoud en de reikwijdte van de rechten van het Handvest die corresponderen met de in het EVRM gegarandeerde rechten, dezelfde zijn als die welke er door genoemd verdrag aan worden toegekend. Terwijl met name voor artikel 7 van het Handvest een equivalent kan worden gevonden in het EVRM, is dit niet het geval voor

[39] HvJ-EU – C-594/12, punten 60 en 61.
[40] HvJ-EU – C-594/12, punt 68.
[41] HvJ-EU – C-594/12, punt 63.
[42] HvJ-EU – C-594/12, punt 64.
[43] HvJ-EU – C-594/12, punt 37.
[44] Europese Toezichthouder voor gegevensbescherming: "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit" (11 april 2017); Europese Toezichthouder voor gegevensbescherming: "Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data" (Richtsnoeren inzake beoordeling van de evenredigheid van maatregelen die het grondrecht op privacy en bescherming van persoonsgegevens beperken), EDPS (19 december 2019).

artikel 8 van het Handvest[45]. Artikel 52, lid 3, van het Handvest verhindert niet dat het recht van de Unie een ruimere bescherming biedt. Aangezien het EVRM geen formeel in het EU-recht opgenomen rechtsinstrument is, moet de EU-wetgeving worden uitgevoerd in het licht van de grondrechten van het Handvest[46].

62. Volgens artikel 8 EVRM mag er bij de uitoefening van dit recht op eerbiediging van het privéleven en het gezinsleven geen inmenging van overheidsdiensten plaatsvinden, behalve wanneer deze bij de wet is voorzien en voor zover deze in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

63. In het EVRM zijn ook normen vastgesteld voor de wijze waarop beperkingen kunnen worden opgelegd. Een van de basisvereisten, naast rechtsstatelijkheid, is voorzienbaarheid. Om te voldoen aan het vereiste van voorzienbaarheid moet het recht voldoende duidelijk zijn in zijn bewoordingen om personen een adequate indicatie te geven van de omstandigheden waarin en de voorwaarden waaronder de overheidsdiensten dergelijke maatregelen kunnen inzetten[47]. Dit vereiste wordt erkend door het HvJ-EU en de EU-wetgeving inzake gegevensbescherming (zie punt 3.2.1.1).

64. De rechten van artikel 8 EVRM worden nader ingevuld in de bepalingen van het Verdrag tot bescherming van personen met betrekking tot de automatische verwerking van persoonsgegevens[48], die ook ten volle moeten worden geëerbiedigd. Hierbij moet echter wel in aanmerking worden genomen dat deze bepalingen slechts een minimumnorm vormen in het licht van het geldende recht van de Unie.

3.2 Specifiek rechtskader – de richtlijn gegevensbescherming bij rechtshandhaving

65. De RGR voorziet in een bepaald kader voor het gebruik van gezichtsherkenningstechnologie. Ten eerste bevat artikel 3, lid 13, van de richtlijn een definitie van de term “biometrische gegevens”[49]. Zie punt 2.1 hierboven voor nadere bijzonderheden. Ten tweede wordt in artikel 8, lid 2, verduidelijkt dat een verwerking alleen rechtmatig is als deze niet alleen noodzakelijk is voor de doeleinden zoals vermeld in artikel 1, lid 1, RGR, maar ook is geregeld in nationale wetgeving waarin ten minste de verwerkingsdoeleinden, de te verwerken persoonsgegevens en de doeleinden van de verwerking worden aangegeven. Andere bepalingen van bijzonder belang met betrekking tot biometrische gegevens zijn de artikelen 10 en 11 RGR. Artikel 10 RGR moet worden gelezen in samenhang met artikel 8 RGR[50]. De beginselen voor de verwerking van persoonsgegevens zoals vastgelegd in artikel 4 van de richtlijn moeten altijd worden nageleefd en moeten bij elke beoordeling van mogelijke biometrische verwerking via gezichtsherkenningstechnologie een leidraad vormen.

---

[45] HvJ-EU – C-203/15 – Tele2 Sverige, punt 129.

[46] HvJ-EU – C-311/18, punt 99.

[47] Europees Hof voor de Rechten van de Mens, arrest, Copland tegen Verenigd Koninkrijk, 3 april 2007, verzoekschrift nr. 62617/00, punt 46.

[48] ETS nr. 108.

[49] Artikel 3, lid 13, RGR: “biometrische gegevens”: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

[50] WP258, Advies inzake een aantal belangrijke aandachtspunten van de richtlijn gegevensbescherming bij rechtshandhaving (Richtlijn (EU) 2016/680), blz. 7.

3.2.1 Verwerking van bijzondere categorieën gegevens voor rechtshandhavingsdoeleinden

66. Volgens artikel 10 RGR is de verwerking van bijzondere categorieën gegevens, zoals biometrische gegevens, alleen toegestaan wanneer de verwerking strikt noodzakelijk is en geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkene. Voor zover geoorloofd op grond van het Unierecht of het lidstatelijk recht, is de verwerking alleen toegestaan om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen, dan wel wanneer die verwerking betrekking heeft op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt. Deze algemene clausule benadrukt de gevoeligheid van de verwerking van bijzondere categorieën gegevens.

3.2.1.1 Toegestaan bij het Unierecht of het lidstatelijk recht

67. Wat het noodzakelijke soort wetgevingsmaatregel betreft, wordt in overweging 33 RGR het volgende gesteld: “Wanneer in deze richtlijn wordt verwezen naar het lidstatelijke recht, een rechtsgrond of een wetgevingsmaatregel, betekent dit niet noodzakelijk dat een door een parlement vastgestelde wetgevingshandeling nodig is, onverminderd de constitutionele vereisten van de betrokken lidstaat.”[51]

68. Volgens artikel 52, lid 1, van het Handvest moeten beperkingen op de uitoefening van de bij het Handvest erkende rechten en vrijheden “bij wet worden gesteld”. Dit sluit aan bij de formulering “voor zover bij de wet is voorzien” in artikel 8, lid 2, EVRM, die niet alleen inhoudt dat het toepasselijke recht moet worden nageleefd, maar ook betrekking heeft op de kwaliteit van dat recht die onverminderd de aard van de handeling verenigbaar moet zijn met de rechtsstaat.

69. In overweging 33 RGR staat verder het volgende: “Dit lidstatelijke recht, die rechtsgrond of die wetgevingsmaatregel moet evenwel duidelijk en nauwkeurig zijn, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is, zoals vereist door de rechtspraak van het Hof van Justitie en het Europees Hof voor de Rechten van de Mens. In het lidstatelijke recht dat de verwerking van persoonsgegevens binnen het toepassingsgebied van deze richtlijn regelt, dienen ten minste de doeleinden, de te verwerken persoonsgegevens en de doeleinden van de verwerking te worden gespecificeerd, alsmede de procedures voor het vrijwaren van de integriteit en de vertrouwelijkheid van persoonsgegevens en de procedures voor de vernietiging ervan.”

70. Het nationale recht moet voldoende duidelijk zijn in zijn bewoordingen om de betrokkenen een adequate indicatie te geven van de omstandigheden waarin en de voorwaarden waaronder de verwerkingsverantwoordelijken dergelijke maatregelen kunnen inzetten. Dit omvat de mogelijke voorwaarden vooraf voor verwerking, zoals specifieke soorten bewijsmateriaal en de noodzaak van gerechtelijke of interne toestemming. Het respectieve recht kan technologieneutraal zijn voor zover er voldoende aandacht is voor de specifieke risico’s en kenmerken van de verwerking van persoonsgegevens door gezichtsherkenningstechnologiesystemen. In overeenstemming met de RGR en de jurisprudentie van het Hof van Justitie van de Europese Unie (HvJ-EU) en het Europees Hof voor de Rechten van de Mens (EHRM), is het inderdaad van wezenlijk belang dat wetgevende maatregelen die als doel hebben een rechtsgrondslag te bieden voor een gezichtsherkenningsmaatregel, voorzienbaar zijn voor de betrokkenen.

71. Indien een wetgevingsmaatregel louter een omzetting is van de algemene bepaling in artikel 10 RGR, kan hierop geen beroep worden gedaan als zijnde een wet die voor rechtshandhavingsdoeleinden de verwerking van biometrische gegevens door middel van gezichtsherkenningstechnologie toestaat.

---

[51] Het soort wetgevingsmaatregelen dat wordt overwogen, moet in overeenstemming zijn met het Unierecht of met het nationale recht. Afhankelijk van de mate van inmenging in de beperking kan op nationaal niveau een bepaalde wetgevingsmaatregel vereist zijn, waarbij rekening wordt gehouden met het niveau van de norm.

72. Naast biometrische gegevens wordt in artikel 10 van de richtlijn de verwerking van andere bijzondere categorieën gegevens geregeld, zoals seksuele gerichtheid, politieke opvattingen en religieuze overtuigingen. Het artikel bestrijkt dus een breed scala van verwerkingen. Bovendien zouden in een dergelijke bepaling de specifieke vereisten ontbreken die aangeven in welke omstandigheden en onder welke voorwaarden rechtshandhavingsinstanties de bevoegdheid zouden hebben om gebruik te maken van gezichtsherkenningstechnologie. Gezien de verwijzing naar andere soorten gegevens en de uitdrukkelijke behoefte aan bijzondere waarborgen zonder nadere specificaties, kan de nationale bepaling tot omzetting van artikel 10 van de richtlijn in nationaal recht, met een vergelijkbare algemene en abstracte formulering, niet worden ingeroepen als rechtsgrondslag voor de verwerking van biometrische gegevens waar gezichtsherkenning bij betrokken is. Een dergelijke bepaling zou immers niet nauwkeurig en voorzienbaar zijn. Overeenkomstig artikel 28, lid 2, of artikel 46, lid 1, punt c), van de richtlijn moet de nationale toezichthoudende autoriteit voor gegevensbescherming worden geraadpleegd voordat de wetgever een nieuwe rechtsgrondslag creëert voor elke vorm van verwerking van biometrische gegevens met behulp van gezichtsherkenning.

3.2.1.2 Strikt noodzakelijk

73. Verwerking kan alleen als "strikt noodzakelijk" worden beschouwd als de inmenging in de bescherming van persoonsgegevens en de beperkingen daarvan beperkt blijven tot wat absoluut noodzakelijk is[52]. De toevoeging van de term "strikt" betekent dat de verwerking van bijzondere categorieën gegevens in de bedoeling van de wetgever alleen mag plaatsvinden onder voorwaarden die nog strikter zijn dan de voorwaarden voor noodzakelijkheid (zie punt 3.1.3.4). Dit moet worden uitgelegd als zijnde een onontkoombare vereiste. Deze beperkt de bij de noodzakelijkheidstoets aan de rechtshandhavingsautoriteit toegestane beoordelingsvrijheid tot een absoluut minimum. In overeenstemming met de vaste rechtspraak van het HvJ-EU is de voorwaarde van "strikte noodzakelijkheid" ook nauw verbonden met het vereiste van objectieve criteria om te bepalen onder welke omstandigheden en voorwaarden de verwerking kan plaatsvinden, waardoor elke verwerking van algemene of systematische aard wordt uitgesloten[53].

3.2.1.3 Kennelijk openbaar gemaakt

74. Bij de beoordeling van de vraag of de verwerking betrekking heeft op gegevens die kennelijk door een betrokkene zelf openbaar zijn gemaakt, moet eraan worden herinnerd dat foto's als zodanig niet systematisch als biometrische gegevens worden beschouwd[54]. Het feit dat een foto kennelijk door de betrokkene zelf openbaar is gemaakt, betekent niet dat de biometrische gegevens uit die foto, die met specifieke technische middelen kunnen worden opgevraagd, worden aangemerkt als kennelijk openbaar gemaakt.

75. Wat persoonsgegevens in het algemeen betreft, moet de betrokkene opzettelijk de biometrische template (en niet louter een gezichtsopname) via een open bron vrij toegankelijk en openbaar hebben gemaakt om biometrische gegevens als kennelijk door de betrokkene zelf openbaar gemaakt te kunnen aanmerken. Als een derde partij de biometrische gegevens openbaar maakt, kan er niet van worden uitgegaan dat de gegevens kennelijk door de betrokkene zelf openbaar zijn gemaakt.

---

[52] Consistente jurisprudentie over het grondrecht op eerbiediging van de persoonlijke levenssfeer, zie HvJ-EU, C-73/07, punt 56 (Satakunnan Markkinapörssi en Satamedia); HvJ-EU, C-92/09 en C-93/09, punt 77 (Schecke en Eifert); HvJ-EU, C-594/12, punt 52 (digitale rechten); HvJ-EU, C-362/14, punt 92 (Schrems).

[53] HvJ-EU, C-623/17, punt 78.

[54] Zie overweging 51 AVG: "De verwerking van foto's mag niet systematisch worden beschouwd als verwerking van bijzondere categorieën persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken."

76. Bovendien is een interpretatie van het gedrag van een betrokkene niet voldoende om biometrische gegevens aan te merken als kennelijk openbaar gemaakt. In het geval van sociale netwerken of onlineplatforms is de EDPB bijvoorbeeld van mening dat het feit dat de betrokkene geen specifieke privacyfuncties heeft geactiveerd of ingesteld, niet volstaat om aan te nemen dat deze betrokkene zijn of haar persoonsgegevens kennelijk zelf openbaar heeft gemaakt en dat deze gegevens (bijv. foto's) zonder toestemming van de betrokkene in biometrische templates kunnen worden omgezet en voor identificatiedoeleinden kunnen worden gebruikt. Meer in het algemeen mogen standaardinstellingen van een dienst, bijv. het openbaar beschikbaar stellen van templates of het ontbreken van een keuze, bijvoorbeeld doordat templates openbaar worden gemaakt zonder dat de gebruiker deze instelling kan wijzigen, op geen enkele manier worden uitgelegd als gegevens die kennelijk openbaar zijn gemaakt.

3.2.2 Geautomatiseerde individuele besluitvorming, waaronder profilering

77. Artikel 11, lid 1, RGR voorziet in de verplichting voor de lidstaten om in het algemeen een verbod in te stellen op besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking, met inbegrip van profilering, en die voor de betrokkene nadelige rechtsgevolgen hebben of hem of haar in aanmerkelijke mate treffen. Als uitzondering op dit algemene verbod kan een dergelijke verwerking alleen mogelijk zijn indien het betrokken besluit is toegestaan krachtens het Unierecht of het lidstatelijke recht dat op de verwerkingsverantwoordelijke van toepassing is, en dat besluit voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkene, waaronder ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke. Uitsluitend een restrictief gebruik ervan is toegestaan. Deze drempel geldt voor gewone (d.w.z. niet bijzondere) categorieën persoonsgegevens. Voor de vrijstelling op grond van artikel 11, lid 2, RGR geldt een nog hogere drempel en een nog restrictiever gebruik. Hiermee wordt nogmaals benadrukt dat besluiten op grond van lid 1 niet mogen worden gebaseerd op bijzondere categorieën gegevens, d.w.z. biometrische gegevens in het bijzonder, om een natuurlijke persoon op unieke wijze te identificeren. In een vrijstelling kan alleen worden voorzien als er passende maatregelen zijn getroffen om de rechten en vrijheden van de betrokkene en de legitieme belangen van de betrokken natuurlijke persoon te beschermen. Deze vrijstelling moet worden gelezen in aanvulling op en in het licht van de uitgangspunten van artikel 10 RGR.

78. Afhankelijk van het gezichtsherkenningstechnologiesysteem biedt mogelijk zelfs de menselijke tussenkomst bij het beoordelen van de resultaten van gezichtsherkenningstechnologie op zich niet noodzakelijkerwijs voldoende garantie voor het eerbiedigen van de rechten van individuen en in het bijzonder het recht op de bescherming van persoonsgegevens, gezien de mogelijke vooringenomenheid en fouten die bij het verwerken zelf kunnen optreden. Bovendien kan de menselijke tussenkomst alleen als een waarborg worden beschouwd als de voor de tussenkomst verantwoordelijke persoon de resultaten van de gezichtsherkenningstechnologie tijdens de menselijke tussenkomst kritisch kan betwisten. Het is van cruciaal belang om de persoon in staat te stellen het gezichtsherkenningstechnologiesysteem en de grenzen ervan te begrijpen en de resultaten ervan naar behoren te interpreteren. Het is ook noodzakelijk om een werkplek en organisatie op te zetten waarin de effecten van vooringenomenheid bij automatisering worden tegengegaan en wordt voorkomen dat een niet-kritische acceptatie van de resultaten wordt bevorderd, bijvoorbeeld door tijdsdruk, omslachtige procedures, mogelijke nadelige gevolgen voor de carrière enz.

79. Krachtens artikel 11, lid 3, RGR, is profilering die leidt tot discriminatie van natuurlijke personen op grond van bijzondere categorieën persoonsgegevens overeenkomstig het Unierecht verboden. Volgens artikel 3, lid 4, van de richtlijn wordt onder "profilering" verstaan elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens

bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling aspecten betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen. Bij het afwegen of is voorzien in passende maatregelen ter bescherming van de rechten en vrijheden van de betrokkene en de legitieme belangen van de betrokken natuurlijke persoon, moet in gedachten worden gehouden dat het gebruik van gezichtsherkenningstechnologie kan leiden tot profilering, afhankelijk van de manier waarop en het doel waarvoor de gezichtsherkenningstechnologie wordt toegepast. In overeenstemming met het Unierecht en artikel 11, lid 3, RGR moet profilering die leidt tot discriminatie van natuurlijke personen op basis van bijzondere categorieën persoonsgegevens, in ieder geval verboden worden.

3.2.3 Categorieën betrokkenen

80. Artikel 6 RGR heeft betrekking op de noodzaak om een onderscheid te maken tussen de verschillende categorieën betrokkenen. Dit onderscheid moet worden gemaakt voor zover dit relevant en mogelijk is. Het moet gevolgen hebben voor de wijze waarop de gegevens worden verwerkt. Uit de voorbeelden in artikel 6 RGR kan worden opgemaakt dat de verwerking van persoonsgegevens in de regel moet voldoen aan de noodzakelijkheids- en evenredigheidscriteria, ook met betrekking tot de categorie betrokkenen[55]. Verder kan hieruit worden opgemaakt dat bij betrokkenen voor wie er geen bewijs is dat erop kan duiden dat er zelfs maar een indirect of gering verband zou kunnen bestaan tussen het gedrag van de betrokkene en het legitieme doel zoals bepaald in de RGR, hoogstwaarschijnlijk geen rechtvaardiging voor inmenging is[56]. Als er geen onderscheid op grond van artikel 6 RGR van toepassing of mogelijk is, moet de uitzondering op de regel van dit artikel ten zeerste in overweging worden genomen bij de beoordeling van de noodzakelijkheid en evenredigheid van de inmenging. Wanneer bij de verwerking van persoonsgegevens gezichtsherkenning wordt gebruikt, is het onderscheiden van verschillende categorieën betrokkenen een essentieel vereiste, ook gezien de mogelijke foutpositieve of foutnegatieve matches die aanzienlijke gevolgen kunnen hebben voor de betrokkenen of in de loop van een onderzoek.

81. Zoals gezegd moeten bij de uitvoering van het Unierecht de bepalingen van het EU-Handvest van de grondrechten worden geëerbiedigd (zie artikel 52 van het Handvest). Het kader en de criteria waarin de RGR voorziet, moeten derhalve worden gelezen in het licht van het Handvest. Rechtshandelingen van de EU en haar lidstaten mogen daar niet bij achterblijven en moeten waarborgen dat het Handvest zijn volle effect sorteert.

3.2.4 Rechten van de betrokkene

82. De EDPB heeft al richtsnoeren verstrekt over verschillende aspecten van de rechten van betrokkenen uit hoofde van de AVG[57]. De richtlijn gegevensbescherming bij rechtshandhaving voorziet in soortgelijke rechten voor betrokkenen, en er zijn algemene richtsnoeren hieromtrent opgesteld in een advies van de Groep gegevensbescherming artikel 29, dat is onderschreven door de EDPB[58]. Onder bepaalde omstandigheden voorziet de RGR in een aantal beperkingen van deze rechten. Op de parameters voor dergelijke beperkingen wordt nader ingegaan in punt 3.2.4.6. “Gerechtvaardigde beperkingen van de rechten van betrokkenen”.

[55] Vgl. ook HvJ-EU, C-594/12, punten 56-59.
[56] Vgl. ook HvJ-EU, C-594/12, punt 58.
[57] Zie bijvoorbeeld Richtsnoeren 1/2022 van de EDPB over de rechten van betrokkenen inzake het recht van inzage (in het Engels) en Richtsnoeren 3/2019 van de EDPB inzake de verwerking van persoonsgegevens door middel van videoapparatuur.
[58] WP258, Advies inzake een aantal belangrijke aandachtspunten van de richtlijn gegevensbescherming bij rechtshandhaving (Richtlijn (EU) 2016/680).

83. Hoewel alle in hoofdstuk III van de RGR vermelde rechten van betrokkenen gezien hun aard ook van toepassing zijn op de verwerking van persoonsgegevens via gezichtsherkenningstechnologie, is het volgende hoofdstuk gericht op enkele rechten en aspecten waarvoor richtsnoeren van bijzonder belang kunnen zijn. Bovendien is dit hoofdstuk en de analyse daarin noodzakelijk voor de vraag of de betreffende verwerking via gezichtsherkenningstechnologie voldoet aan de in het vorige hoofdstuk beschreven wettelijke vereisten.

84. Gezien de aard van de verwerking van persoonsgegevens via gezichtsherkenningstechnologie (verwerking van speciale categorieën persoonsgegevens, vaak zonder duidelijke interactie met de betrokkene) moet de verwerkingsverantwoordelijke, voordat de verwerking via gezichtsherkenningstechnologie van start gaat, zorgvuldig overwegen hoe (en of) aan de vereisten van de RGR kan worden voldaan. Met name door zorgvuldige analyse van het volgende:

- wie de betrokkenen zijn (vaak meer dan de degene(n) die het hoofddoel van de verwerking vormen);
- hoe de betrokkenen op de hoogte worden gesteld van de verwerking via gezichtsherkenningstechnologie (zie punt 3.2.4.1);
- hoe de betrokkenen hun rechten kunnen uitoefenen (hierbij kunnen zowel informatie- en inzagerechten als het recht op rectificatie of beperking bijzonder moeilijk te handhaven zijn wanneer de gezichtsherkenningstechnologie wordt gebruikt voor alle verificaties behalve de één-op-éénverificatie, waarbij er direct contact met de betrokkene is).

3.2.4.1 Betrokkenen op de hoogte stellen van de rechten en informatie in een beknopte, begrijpelijke en gemakkelijk toegankelijke vorm

85. Bij gezichtsherkenningstechnologie kan het moeilijk zijn om ervoor te zorgen dat betrokkenen op de hoogte worden gesteld van de verwerking van hun biometrische gegevens. Het is met name moeilijk wanneer een rechtshandhavingsinstantie met behulp van gezichtsherkenningstechnologie videomateriaal analyseert dat afkomstig is van of wordt verstrekt door een derde. De rechtshandhavingsinstantie heeft immers weinig en meestal geen mogelijkheid om de betrokkene in kennis te stellen op het moment van de verzameling (bijv. via een bord ter plaatse). Voordat de verwerking van biometrische gegevens wordt uitgevoerd, moet het videomateriaal dat niet relevant is voor het onderzoek (of het doel voor de verwerking) altijd worden verwijderd of geanonimiseerd (bijv. door het onscherp te maken, zonder de mogelijkheid de gegevens later te herstellen) om het risico te vermijden dat niet is voldaan aan het beginsel van minimale gegevensverwerking in artikel 4, lid 1, punt e), RGR en de informatieverplichtingen in artikel 13, lid 2, RGR. Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om te beoordelen welke informatie voor de betrokkene van belang zou kunnen zijn bij de uitoefening van zijn of haar rechten en om ervoor te zorgen dat de noodzakelijke informatie wordt verstrekt. De doeltreffende uitoefening van de rechten van de betrokkene is afhankelijk van de naleving van de informatieverplichtingen door de verwerkingsverantwoordelijke.

86. In artikel 13, lid 1, RGR is bepaald welke minimuminformatie in het algemeen aan de betrokkene moet worden verstrekt. Deze informatie kan worden verstrekt via de website van de verwerkingsverantwoordelijke, in gedrukte vorm (bijv. een op verzoek beschikbare brochure) of via anderszins gemakkelijk toegankelijke bronnen voor de betrokkene. De verwerkingsverantwoordelijke moet in elk geval ervoor zorgen dat er op doelmatige wijze informatie wordt verstrekt over ten minste de volgende onderdelen:

- de identiteit en de contactgegevens van de verwerkingsverantwoordelijke, waaronder die van de functionaris voor gegevensbescherming;
- de doeleinden van de verwerking en dat de verwerking via gezichtsherkenningstechnologie plaatsvindt;
- het recht om een klacht in te dienen bij een toezichthoudende autoriteit en de contactgegevens van die autoriteit;
- het recht om te verzoeken om toegang tot en rectificatie of wissing van persoonsgegevens en beperking van de verwerking van de persoonsgegevens.

87. Daarnaast moet in specifieke gevallen, zoals vastgesteld in het nationale recht dat in overeenstemming moet zijn met artikel 13, lid 2, RGR[59], zoals bijvoorbeeld de verwerking via gezichtsherkenningstechnologie, de volgende informatie rechtstreeks aan de betrokkene worden verstrekt:
    - de rechtsgrond van de verwerking;
    - informatie over de plaats waar de persoonsgegevens zonder medeweten van de betrokkene zijn verzameld;
    - de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
    - in voorkomend geval, de categorieën van ontvangers van de persoonsgegevens (met inbegrip van derde landen of internationale organisaties).

88. Terwijl artikel 13, lid 1, RGR betrekking heeft op algemene informatie die aan het publiek beschikbaar wordt gesteld, heeft artikel 13, lid 2, RGR betrekking op de aanvullende informatie die in specifieke gevallen aan een bepaalde betrokkene moet worden verstrekt, bijvoorbeeld wanneer de gegevens direct bij de betrokkene of indirect zonder medeweten van de betrokkene worden verzameld[60]. Er is geen duidelijke definitie van wat wordt verstaan onder “specifieke gevallen” in artikel 13, lid 2, RGR. De bepaling verwijst echter naar situaties waarin de betrokkenen op de hoogte moeten worden gesteld van de specifiek op hen betrekking hebbende verwerking en passende informatie moeten krijgen om doeltreffend hun rechten te kunnen uitoefenen. De EDPB is van mening dat bij de beoordeling van de vraag of er sprake is van een “specifiek geval” verschillende factoren in aanmerking moeten worden genomen, waaronder of de persoonsgegevens worden verzameld zonder dat de betrokkene hiervan op de hoogte is. Dit zou immers de enige manier zijn waarop betrokkenen doeltreffend hun rechten kunnen uitoefenen. Andere voorbeelden van “specifieke gevallen” zijn gevallen waarbij de persoonsgegevens verder worden verwerkt in het kader van een internationale strafrechtelijke samenwerkingsprocedure of waarbij persoonsgegevens worden verwerkt in het kader van geheime operaties zoals vastgesteld in de nationale wetgeving. Voorts volgt uit overweging 38 RGR dat, indien de besluitvorming uitsluitend op basis van gezichtsherkenningstechnologie plaatsvindt, de betrokkenen op de hoogte moeten worden gesteld van de kenmerken van de geautomatiseerde

[59] Bijvoorbeeld artikel 56, lid 1, van de Duitse federale gegevensbeschermingswet, waarin onder meer wordt bepaald welke informatie aan betrokkenen moet worden verstrekt bij undercoveractiviteiten.
[60] WP258, Advies inzake een aantal belangrijke aandachtspunten van de richtlijn gegevensbescherming bij rechtshandhaving (Richtlijn (EU) 2016/680), blz. 17-18.

besluitvorming. Dit zou er ook op wijzen dat dit een specifiek geval is waarin overeenkomstig artikel 13, lid 2, RGR aanvullende informatie aan de betrokkene moet worden verstrekt[61].

89. Tot slot moet worden opgemerkt dat de lidstaten overeenkomstig artikel 13, lid 3, RGR wettelijke maatregelen kunnen vaststellen waarin de verplichting tot het verstrekken van informatie in specifieke gevallen voor bepaalde doelstellingen wordt beperkt. Dit geldt voor zover en zolang een dergelijke maatregel een noodzakelijke en evenredige maatregel is in een democratische samenleving, met inachtneming van de grondrechten en de gerechtvaardigde belangen van de betrokkene.

3.2.4.2 Recht van inzage

90. In het algemeen heeft de betrokkene recht op een positieve of negatieve bevestiging van de verwerking van zijn of haar persoonsgegevens en, indien het antwoord positief is, op de toegang tot de persoonsgegevens als zodanig, plus aanvullende informatie, zoals vermeld in artikel 14 RGR. Wanneer bij gezichtsherkenningstechnologie de biometrische gegevens ook door middel van alfanumerieke gegevens worden opgeslagen en aan een identiteit worden gekoppeld, moet de bevoegde autoriteit een verzoek om inzage kunnen bevestigen op basis van een zoekopdracht aan de hand van die alfanumerieke gegevens, zonder verdere verwerking van biometrische gegevens van anderen (d.w.z. door met gezichtsherkenningstechnologie te zoeken in een database). Het beginsel van gegevensminimalisering moet in acht worden genomen en er mogen niet meer gegevens worden opgeslagen dan noodzakelijk is met betrekking tot het doel van de verwerking.

3.2.4.3 Recht op rectificatie van persoonsgegevens

91. Aangezien gezichtsherkenningstechnologie geen absolute nauwkeurigheid biedt, is het van bijzonder belang dat verwerkingsverantwoordelijken alert zijn op verzoeken om rectificatie van persoonsgegevens. Dit kan ook het geval zijn wanneer een betrokkene op basis van de gezichtsherkenningstechnologie in een onjuiste categorie is ingedeeld, bijv. wanneer hij/zij ten onrechte in de categorie verdachten is ingedeeld op basis van een eerste aanname van de handelwijze in videobeelden. De risico's voor de betrokkenen zijn met name ernstig indien dergelijke onjuiste gegevens worden opgeslagen in een politiedatabase en/of worden gedeeld met andere entiteiten. De verwerkingsverantwoordelijke moet de opgeslagen gegevens en de systemen voor gezichtsherkenningstechnologie dienovereenkomstig corrigeren; zie overweging 47 RGR.

3.2.4.4 Recht op gegevenswissing

92. Wanneer gezichtsherkenningstechnologie niet wordt gebruikt voor één-op-éénverificatie/authenticatie, zal er in de meeste gevallen sprake zijn van het verwerken van de biometrische gegevens van een groot aantal betrokkenen. Het is daarom belangrijk dat de verwerkingsverantwoordelijke vooraf de beperkingen voor het doel en de noodzaak nagaat, zodat een verzoek om wissing overeenkomstig artikel 16 RGR zonder onnodige vertraging kan worden behandeld. De verwerkingsverantwoordelijke moet immers onder meer persoonsgegevens wissen waarvan de verwerking verder gaat dan wat in de toepasselijke wetgeving op grond van de artikelen 4, 8 en 10 RGR is toegestaan.

3.2.4.5 Recht op beperking

93. Indien de juistheid van de gegevens door de betrokkene wordt betwist en de juistheid van de gegevens niet kan worden vastgesteld (of wanneer de persoonsgegevens moeten worden bewaard met het oog op toekomstig bewijsmateriaal), is de verwerkingsverantwoordelijke overeenkomstig artikel 16 RGR

[61] Let op het verschil tussen "aan de betrokkene ter beschikking gesteld" in artikel 13, lid 1, RGR en "verstrekken aan de betrokkene" in artikel 13, lid 2, RGR. In artikel 13, lid 2, RGR moet de verwerkingsverantwoordelijke ervoor zorgen dat de informatie de betrokkene bereikt, waarbij het niet voldoende is om de informatie op een website te publiceren.

verplicht de persoonsgegevens van die betrokkene te beperken. Dit wordt met name belangrijk bij het gebruik van gezichtsherkenningstechnologie (die uitgaat van een of meer algoritmen en dus nooit een doorslaggevend resultaat laat zien) in situaties waarin grote hoeveelheden gegevens worden verzameld en de nauwkeurigheid en kwaliteit van de identificatie kunnen variëren. Bij videomateriaal van slechte kwaliteit (bijv. van een plaats delict) neemt het risico op foutpositieven toe. Als gezichtsfoto's in een volglijst niet regelmatig worden bijgewerkt, verhoogt dat bovendien het risico op foutpositieven of foutnegatieven. In specifieke gevallen, wanneer gegevens niet kunnen worden gewist omdat er redelijke gronden zijn om aan te nemen dat het wissen van de gegevens de legitieme belangen van de betrokkene zou kunnen schaden, moeten de gegevens in plaats daarvan worden beperkt en alleen worden verwerkt voor het doel dat aan het wissen in de weg staat (zie overweging 47 RGR).

3.2.4.6 Gerechtvaardigde beperkingen van de rechten van de betrokkene

94. Bij de informatieverplichtingen van de verwerkingsverantwoordelijke en het recht van inzage van de betrokkenen zijn beperkingen alleen toegestaan als ze zijn vastgelegd in de wet, die op haar beurt een noodzakelijke en evenredige maatregel in een democratische samenleving moet zijn waarin de grondrechten en de gerechtvaardigde belangen van de natuurlijke persoon in kwestie in acht worden genomen (zie artikel 13, lid 3, artikel 13, lid 4, artikel 15 en artikel 16, lid 4, RGR). Wanneer gezichtsherkenningstechnologie wordt gebruikt voor rechtshandhavingsdoeleinden, kan men verwachten dat het wordt gebruikt onder omstandigheden waarin het voor het nagestreefde doel schadelijk zou zijn om de betrokkene te informeren of inzage in de gegevens te verlenen. Dit geldt bijvoorbeeld voor een politieonderzoek naar een strafbaar feit of om de nationale of openbare veiligheid te beschermen.

95. Het recht op inzage betekent niet automatisch inzage in alle informatie, bijvoorbeeld in een strafzaak waarin iemands persoonsgegevens voorkomen. Een bruikbaar voorbeeld van wanneer beperkingen van het recht toegestaan zouden kunnen zijn, is gedurende een strafrechtelijk onderzoek.

3.2.4.7 Uitoefening van rechten via de toezichthoudende autoriteit

96. In gevallen waarin er legitieme beperkingen zijn op de uitoefening van rechten overeenkomstig hoofdstuk III van de RGR, kan de betrokkene de gegevensbeschermingsautoriteit verzoeken de rechten namens hem of haar uit te oefenen door de rechtmatigheid van de verwerking door de verwerkingsverantwoordelijke te controleren. Het is aan de verwerkingsverantwoordelijke om de betrokkene in kennis te stellen van de mogelijkheid om de rechten op een dergelijke manier uit te oefenen (zie artikel 17 RGR en artikel 46, lid 1, punt g), RGR). Voor de gezichtsherkenningstechnologie betekent dit dat de verwerkingsverantwoordelijke ervoor moet zorgen dat er passende maatregelen zijn getroffen zodat een dergelijk verzoek kan worden behandeld, bijvoorbeeld door het mogelijk te maken opgenomen materiaal te doorzoeken, op voorwaarde dat de betrokkene voldoende informatie verstrekt om zijn of haar persoonsgegevens te lokaliseren.

3.2.5 Andere wettelijke vereisten en waarborgen

3.2.5.1 Artikel 27 Gegevensbeschermingseffectbeoordeling (PEB)

97. Voorafgaand aan het gebruik van gezichtsherkenningstechnologie is een PEB een essentiële eis aangezien het soort verwerking, in het bijzonder wanneer daarbij nieuwe technologieën worden gebruikt, gelet op de aard, de reikwijdte, de context of de doeleinden daarvan, waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert. Aangezien het gebruik van de gezichtsherkenningstechnologie gepaard gaat met de systematische automatische verwerking van bijzondere categorieën gegevens, mag worden aangenomen dat in dergelijke gevallen de verwerkingsverantwoordelijke in de regel verplicht zou zijn om een PEB uit te voeren. De PEB bevat

ten minste een algemene beschrijving van de beoogde verwerkingen, een beoordeling van de noodzaak en evenredigheid van de verwerkingsactiviteiten in relatie tot de doeleinden, een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen, de beoogde maatregelen ter beperking van de risico's, de voorzorgsmaatregelen, de beveiligingsmaatregelen en de mechanismen die zijn ingesteld om de persoonsgegevens te beschermen en aan te tonen dat aan deze richtlijn is voldaan. De EDPB beveelt aan om de resultaten van dergelijke beoordelingen, of ten minste de belangrijkste bevindingen en conclusies van de PEB, openbaar te maken als een maatregel ter bevordering van vertrouwen en transparantie[62].

3.2.5.2 Artikel 28 Voorafgaande raadpleging van de toezichthoudende autoriteit

98. Op grond van artikel 28 RGR moet de verwerkingsverantwoordelijke of de verwerker de toezichthoudende autoriteit voorafgaand aan de verwerking raadplegen wanneer: a) uit een PEB blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken; of b) de aard van de verwerking, in het bijzonder wanneer wordt gebruikgemaakt van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van betrokkenen inhoudt. Zoals reeds uiteengezet in punt 2.3 van deze richtsnoeren, is de EDPB van mening dat de meeste gevallen waarin gezichtsherkenningstechnologie wordt ingezet en gebruikt, een intrinsiek hoog risico inhouden voor de rechten en vrijheden van betrokkenen. Naast de PEB moet de autoriteit die de gezichtsherkenningstechnologie gebruikt, voorafgaand aan het gebruiken van het systeem daarom ook de bevoegde toezichthoudende autoriteit raadplegen.

3.2.5.3 Artikel 29 Beveiliging van de verwerking

99. Door de unieke aard van biometrische gegevens is het voor een betrokkene onmogelijk om de gegevens te wijzigen wanneer ze worden aangetast, bijvoorbeeld als gevolg van een gegevensinbreuk. Daarom moet de bevoegde autoriteit die de gezichtsherkenningstechnologie uitvoert en/of gebruikt, bijzondere aandacht besteden aan de beveiliging van de verwerking, overeenkomstig artikel 29 RGR. De rechtshandhavingsautoriteit moet er met name voor zorgen dat het systeem voldoet aan de relevante normen en moet maatregelen treffen om de biometrische templates te beschermen[63]. Deze verplichting is des te relevanter wanneer de rechtshandhavingsautoriteit gebruikmaakt van een externe dienstverlener (gegevensverwerker).

3.2.5.4 Artikel 20 Gegevensbescherming door ontwerp en door standaardinstellingen

100. Overeenkomstig artikel 20 RGR heeft gegevensbescherming door ontwerp en door standaardinstellingen tot doel ervoor te zorgen dat de gegevensbeschermingsbeginselen, zoals gegevensminimalisatie en opslagbeperking, al voor de aanvang van de verwerking via passende technische en organisatorische maatregelen, zoals pseudonimisering, zijn ingebouwd in de technologie en gedurende de hele levenscyclus van de gegevens worden toegepast. Gezien het inherente hoge risico voor de rechten en vrijheden van natuurlijke personen, moet de keuze van dergelijke maatregelen niet alleen afhangen van economische overwegingen[64], maar moet ernaar worden gestreefd de meest geavanceerde gegevensbeschermingstechnologieën toe te passen. In dezelfde trant moet een rechtshandhavingsinstantie, wanneer deze voornemens is gezichtsherkenningstechnologie van externe aanbieders toe te passen en te gebruiken, ervoor zorgen

[62] Zie voor meer informatie WP248 rev.01 Richtsnoeren betreffende gegevensbeschermingseffectbeoordeling en om te bepalen of de verwerking "waarschijnlijk een hoog risico inhoudt".
[63] Zie bijvoorbeeld: ISO/IEC 24745 Information security, cybersecurity and privacy protection – Biometric information protection (Informatiebeveiliging, cyberbeveiliging en bescherming van de privacy – Bescherming van biometrische gegevens).
[64] Zie overweging 53 RGR.

dat alleen gezichtsherkenningstechnologie wordt ingezet die is ontwikkeld op basis van de beginselen van gegevensbescherming door ontwerp en door standaardinstellingen[65]. Dit betekent ook dat de transparantie over de werking van gezichtsherkenningstechnologie niet beperkt wordt door claims van bedrijfsgeheimen of intellectuele eigendomsrechten.

3.2.5.5 Artikel 25 Bijhouden van logbestanden

101. De RGR bevat verschillende methoden om de rechtmatigheid van de verwerking door de verwerkingsverantwoordelijke of de verwerker aan te tonen en de integriteit en de beveiliging van de gegevens te waarborgen. In dit opzicht zijn logbestanden in het systeem een zeer nuttig instrument en een belangrijke waarborg voor de verificatie van de rechtmatigheid van de verwerking, zowel intern (d.w.z. zelfcontrole) als door externe toezichthoudende autoriteiten, zoals de gegevensbeschermingsautoriteiten. Overeenkomstig artikel 25 RGR moeten logbestanden worden bijgehouden van ten minste de volgende verwerkingen in systemen voor geautomatiseerde verwerking: verzameling, wijziging, raadpleging, bekendmaking onder meer in de vorm van doorgiften, combinatie en wissing. Bovendien moeten de logbestanden van raadpleging en bekendmakingen het mogelijk maken de redenen, de datum en het tijdstip van die handelingen te achterhalen en indien mogelijk de identiteit van de persoon die persoonsgegevens heeft geraadpleegd of bekendgemaakt, en de identiteit van de ontvangers van die persoonsgegevens. Voorts wordt, in de context van gezichtsherkenningssystemen, registratie van de volgende aanvullende verwerkingsactiviteiten aanbevolen (deels buiten artikel 25 RGR):

- wijzigingen in de referentiedatabase (toevoeging, verwijdering of bijwerking) – wanneer het niet mogelijk is om de rechtmatigheid of het resultaat van de verwerkingen op een andere manier te controleren, moet in het logbestand een kopie van de betrokken (toegevoegde, verwijderde of bijgewerkte) afbeelding worden bewaard;

- pogingen tot identificatie of verificatie, met inbegrip van het resultaat en de betrouwbaarheidsscore – het beginsel van strikte minimalisering moet worden toegepast, zodat alleen de identificatiecode van de afbeelding uit de referentiedatabase in de logbestanden wordt bewaard en niet de hele referentieafbeelding wordt opgeslagen, en logbestanden met de ingevoerde biometrische gegevens moeten worden vermeden, tenzij dit noodzakelijk is (bijv. alleen in gevallen waarin er een match is);

- de ID van de gebruiker die om de identificatie- of verificatiepoging heeft verzocht;

- de in de logbestanden van de systemen opgeslagen persoonsgegevens zijn onderworpen aan strikte beperkingen ten aanzien van het doel (bijv. audits) en mogen niet voor andere doeleinden worden gebruikt (bijv. om alsnog herkenning/verificatie te kunnen uitvoeren van een afbeelding die uit de referentiedatabase is verwijderd). Er moeten beveiligingsmaatregelen worden getroffen om de integriteit van de logbestanden te waarborgen, waarbij automatische bewakingssystemen om misbruik van logbestanden op te sporen ten zeerste worden aanbevolen. Wanneer er gezichtsopnames worden opgeslagen, moeten de beveiligingsmaatregelen voor de logbestanden van de referentiedatabase gelijkwaardig zijn aan die voor de referentiedatabase. Ook moeten automatische processen worden ingevoerd om de handhaving van de bewaringstermijn voor de logbestanden te waarborgen.

[65] Zie voor meer informatie de Richtsnoeren van de EDPB inzake gegevensbescherming door ontwerp en door standaardinstellingen: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf .

3.2.5.6 Artikel 4, lid 4 Verantwoordingsplicht

102. De verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerking voldoet aan de beginselen van artikel 4, leden 1, 2 en 3 (zie artikel 4, lid 4, RGR). Een systematische en actuele documentatie van het systeem (inclusief actualiseringen, upgrades en algoritmische training), de technische en organisatorische maatregelen (waaronder bewaking van de systeemprestaties en mogelijke menselijke tussenkomst) en de verwerking van de persoonsgegevens zijn in dit verband cruciaal. Om de rechtmatigheid van de verwerking aan te tonen, is het bijhouden van logbestanden overeenkomstig artikel 25 RGR een bijzonder belangrijk element (zie punt 3.2.5.5). Het verantwoordingsbeginsel heeft niet alleen betrekking op het systeem en de verwerking, maar ook op de documentatie van procedurele waarborgen zoals noodzakelijkheids- en evenredigheidsbeoordelingen, gegevensbeschermingseffectbeoordelingen en interne raadplegingen (bijv. goedkeuring van het project door het management of interne besluiten over de waarden voor betrouwbaarheidsscores) en externe raadplegingen (bijv. gegevensbeschermingsautoriteiten). Bijlage II bevat een aantal elementen in dit verband.

3.2.5.7 Artikel 47 Doeltreffend toezicht

103. Doeltreffend toezicht door de bevoegde gegevensbeschermingsautoriteiten is een van de belangrijkste waarborgen voor de rechten en vrijheden van de personen die te maken krijgen met het gebruik van gezichtsherkenningstechnologie. Tegelijkertijd is het voor de doeltreffende uitvoering van hun taken en de uitoefening van hun bevoegdheden een voorwaarde dat aan elke gegevensbeschermingsautoriteit de benodigde personele, technische en financiële middelen, gebouwen en infrastructuur worden verstrekt[66]. Nog belangrijker dan het aantal beschikbare personeelsleden zijn de vaardigheden van de deskundigen, die een zeer breed scala aan onderwerpen moeten bestrijken, van strafrechtelijke onderzoeken en politiële samenwerking tot big data-analyse en AI. Daarom moeten de lidstaten ervoor zorgen dat de toezichthoudende autoriteiten over passende en voldoende middelen beschikken om hun mandaat inzake de bescherming van de rechten van de betrokkenen te kunnen vervullen en moeten zij de ontwikkelingen op dit gebied nauwlettend volgen[67].

4 CONCLUSIE

104. Het gebruik van gezichtsherkenningstechnologieën is onlosmakelijk verbonden met de verwerking van aanzienlijke hoeveelheden persoonsgegevens, waaronder bijzondere categorieën gegevens. Het gezicht en, meer in het algemeen, biometrische gegevens zijn permanent en onherroepelijk verbonden met iemands identiteit. Daarom heeft het gebruik van gezichtsherkenning direct of indirect invloed op een aantal rechten en vrijheden die zijn vastgelegd in het Handvest van de grondrechten van de EU en die verder kunnen gaan dan privacy en gegevensbescherming, zoals menselijke waardigheid, vrijheid van verkeer, vrijheid van vergadering en andere. Dit is met name van belang op het gebied van rechtshandhaving en strafrecht.

105. De EDPS begrijpt dat het nodig is dat rechtshandhavingsinstanties moeten kunnen profiteren van de best mogelijke instrumenten om snel de identiteit van daders van terroristische handelingen en andere ernstige strafbare feiten te achterhalen. Dergelijke instrumenten moeten echter worden gebruikt in

[66] Zie de mededeling van de Commissie Eerste verslag over de toepassing en werking van Richtlijn (EU) 2016/680, de richtlijn gegevensbescherming bij rechtshandhaving ("richtlijn rechtshandhaving"), COM(2022) 364 final, punt 3.4.1.

[67] Zie de bijdrage van de EDPB aan de evaluatie door de Europese Commissie van de richtlijn gegevensbescherming bij rechtshandhaving op grond van artikel 62, lid 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

strikte overeenstemming met het toepasselijke rechtskader en alleen in gevallen waarin zij voldoen aan de vereisten van noodzakelijkheid en evenredigheid, zoals bepaald in artikel 52, lid 1, van het Handvest. Hoewel een deel van de oplossing is gelegen in moderne technologieën, zijn deze geenszins een wondermiddel.

106. Er zijn bepaalde toepassingen van technologieën voor gezichtsherkenning die onaanvaardbaar hoge risico's inhouden voor personen en de samenleving ("rode lijnen"). Om deze redenen hebben de EDPB en de EDPS opgeroepen tot een algemeen verbod[68].

107. Met name de biometrische identificatie op afstand van personen in openbaar toegankelijke ruimten vormt een hoog risico op inmenging in het privéleven van personen en hoort niet thuis in een democratische samenleving, aangezien deze, gelet op de aard ervan, massasurveillance inhoudt. In dezelfde geest is de EDPB van mening dat door AI ondersteunde gezichtsherkenningssystemen die personen op basis van hun biometrische kenmerken indelen in clusters op basis van etniciteit, geslacht, politieke of seksuele gerichtheid, niet verenigbaar zijn met het Handvest. Voorts is de EDPB ervan overtuigd dat het gebruik van gezichtsherkenningstechnologie of vergelijkbare technologieën om emoties van een natuurlijk persoon af te leiden, zeer onwenselijk is en verboden zou moeten worden, mogelijk met enkele naar behoren gerechtvaardigde uitzonderingen. Daarnaast is de EDPB van mening dat het in het kader van rechtshandhaving verwerken van persoonsgegevens waarbij gebruik wordt gemaakt van een database die is gevuld door massaal en zonder onderscheid persoonsgegevens te verzamelen, bijvoorbeeld door het "scrapen" van online toegankelijke foto's en gezichtsopnamen, in het bijzonder die welke via sociale netwerken beschikbaar zijn gesteld, als zodanig niet zou voldoen aan de strikte noodzakelijkheidseis waarin het recht van de Unie voorziet.

5 BIJLAGEN

Bijlage I: Ondersteuningspatroon

Bijlage II: Praktische richtsnoeren voor het beheer van projecten op het gebied van gezichtsherkenningstechnologie in rechtshandhavingsinstanties

Bijlage III: Praktische voorbeelden

[68] Zie gezamenlijk advies 5/2021 van de EDPB en de EDPS over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet inzake artificiële intelligentie): https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

BIJLAGE I – SJABLOON VOOR DE BESCHRIJVING VAN SCENARIO'S

(Met informatiekaders voor aspecten die binnen het scenario worden behandeld)

Beschrijving van de verwerking:

- Beschrijving van de verwerking, context (verband met strafbaar feit), doel

Bron van de informatie:

- Soorten betrokkenen: ☐ alle burgers ☐ veroordeelden ☐verdachten ☐ kinderen ☐ andere kwetsbare betrokkenen
- Bron van de afbeelding: ☐ openbaar toegankelijke ruimten ☐ internet ☐ particuliere entiteit☐ andere personen ☐ overig .....
- Verband met strafbaar feit: ☐ direct temporeel ☐ niet direct temporeel ☐ direct geografisch ☐ niet direct geografisch ☐ niet noodzakelijk
- Wijze waarop de informatie is vastgelegd: ☐ op afstand ☐ in een cabine of in een gecontroleerde omgeving
- Context, gevolgen voor andere grondrechten:
  ☐ Nee
  Ja, te weten ☐ vrijheid van vergadering
  ☐ vrijheid van meningsuiting
  ☐ verscheidene:.....
- Mogelijkheden voor aanvullende informatiebronnen over de betrokkene:
  ☐ identiteitsbewijs ☐ gebruik van openbare telefoon ☐ kentekenplaat van het voertuig
  ☐ overig .....

Referentiedatabase (waarmee de vastgelegde informatie wordt vergeleken):

- Specifiek karakter: ☐ databases voor algemene doeleinden ☐ specifieke databases op misdaadgebied
- Beschrijving van de wijze waarop deze referentiedatabases zijn gevuld (en de rechtsgrondslag)
- Wijziging van het doel van de database (bijv. het primaire doel was de beveiliging van particuliere eigendommen): ☐ JA ☐ NEE

Algoritme:

- Soort verwerking: ☐ één-op-éénverificatie (authenticatie)☐ één-op-velenidentificatie
- Overwegingen in verband met de nauwkeurigheid
- Technische waarborgen

Resultaat:

- Effect ☐ direct (de betrokkene kan bijvoorbeeld worden gearresteerd of ondervraagd, discriminerend gedrag)

  ☐ niet direct (wordt gebruikt voor statistische modellen, geen juridische actie van betekenis tegen betrokkenen)

- Geautomatiseerde beslissing: ☐ JA ☐ NEE
- Duur van de opslag

Juridische analyse:

- Analyse van de noodzakelijkheid en evenredigheid – doel/ernst van het strafbaar feit/aantal personen dat niet bij de verwerking is betrokken maar er wel door wordt getroffen
- Soort voorafgaande informatie aan de betrokkene: ☐ bij het betreden van het specifieke gebied

  ☐ op de website van de rechtshandhavingsinstantie in het algemeen

  ☐ op de website van de rechtshandhavingsinstantie voor de specifieke verwerking

  ☐ overig .....
- Toepasselijk rechtskader:

  ☐ RGR grotendeels overgenomen in nationaal recht

  ☐ algemene nationale wetgeving inzake het gebruik van biometrische gegevens door rechtshandhavingsinstanties

  ☐ bijzondere nationale wetgeving voor deze verwerking (gezichtsherkenning) voor de betreffende bevoegde autoriteit

  ☐ bijzondere nationale wetgeving voor deze verwerking (geautomatiseerde beslissing)

Conclusie:

Algemene overwegingen met betrekking tot de vraag of de beschreven verwerking waarschijnlijk verenigbaar is met het Unierecht (en enkele verwijzingen naar wettelijke vereisten)

BIJLAGE II – PRAKTISCHE RICHTSNOEREN VOOR HET BEHEER VAN PROJECTEN OP HET GEBIED VAN GEZICHTSHERKENNINGSTECHNOLOGIE IN RECHTSHANDHAVINGSINSTANTIES

Deze bijlage bevat enkele aanvullende praktische richtsnoeren voor rechtshandhavingsinstanties die voornemens zijn een project met betrekking tot gezichtsherkenningstechnologie op te starten. De bijlage bevat meer informatie over de organisatorische en technische maatregelen die tijdens de uitvoering van het project in aanmerking moeten worden genomen en mag niet worden beschouwd als een uitputtende lijst van te nemen stappen/maatregelen. De bijlage moet ook worden gezien in samenhang met de Richtsnoeren 3/2019 van de EDPB inzake de verwerking van persoonsgegevens door middel van videoapparatuur[69] en de regelgeving in de EU/EER en de richtsnoeren van de EDPB met betrekking tot het gebruik van artificiële intelligentie.

Bij de richtsnoeren in deze bijlage is uitgegaan van de veronderstelling dat rechtshandhavingsinstanties gezichtsherkenningstechnologie zullen aankopen (als kant-en-klare producten). Als de rechtshandhavingsinstantie voornemens is de gezichtsherkenningstechnologie te ontwikkelen (verder te trainen), gelden aanvullende eisen voor het selecteren van de benodigde trainings-, validatie- en testdatasets die tijdens de ontwikkeling moeten worden gebruikt en de rollen/maatregelen voor de ontwikkelomgeving. Ook bij een kant-en-klaar product kunnen verdere aanpassingen nodig zijn voor het beoogde gebruik, in welk geval moet worden voldaan aan de bovengenoemde vereisten voor de selectie van test-, validatie- en trainingsdatasets.

Het feit dat iemand tot dezelfde rechtshandhavingsinstantie behoort, biedt op zichzelf geen volledige toegang tot biometrische gegevens. Net als bij andere categorieën persoonsgegevens kunnen biometrische gegevens die op basis van een specifieke rechtsgrondslag zijn verzameld voor een bepaald rechtshandhavingsdoel niet zonder passende rechtsgrondslag voor een ander rechtshandhavingsdoel worden gebruikt (artikel 4, lid 2, van Richtlijn (EU) 2016/680 (RGR)). Het ontwikkelen/trainen van een instrument voor gezichtsherkenningstechnologie wordt ook als een ander doel beschouwd, waarbij moet worden beoordeeld of het verwerken van biometrische gegevens om de prestaties te meten of de technologie te trainen en daarmee te voorkomen dat de betrokken de gevolgen ondervinden van slechte prestaties, noodzakelijk en evenredig is, rekening houdend met het oorspronkelijke doel van de verwerking.

1. ROLLEN EN VERANTWOORDELIJKHEDEN

Wanneer een rechtshandhavingsinstantie gezichtsherkenningstechnologie inzet voor de uitvoering van taken die onder het toepassingsgebied van de richtlijn gegevensbescherming bij rechtshandhaving vallen (de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten enz. overeenkomstig artikel 3 RGR), kan deze worden beschouwd als de verwerkingsverantwoordelijke voor de gezichtsherkenningstechnologie. Rechtshandhavingsinstanties bestaan echter uit verschillende eenheden/afdelingen die bij deze verwerking betrokken kunnen zijn, hetzij door de procedure voor toepassing van gezichtsherkenningstechnologie vast te stellen of door de technologie in de praktijk te gebruiken. Vanwege de specifieke kenmerken van deze technologie moeten er

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

mogelijk verschillende eenheden worden ingeschakeld om ondersteuning bij het meten van de prestaties te bieden of om de technologie verder te trainen.

Bij een project op het gebied van gezichtsherkenningstechnologie zijn er verschillende belanghebbenden[70] binnen de rechtshandhavingsinstanties die mogelijk betrokken moeten worden:

- Hoger management: het project goedkeuren na afweging van de risico's tegen de potentiële voordelen.
- Functionaris voor gegevensbescherming en/of juridische afdeling van de rechtshandhavingsinstantie: assisteren bij de beoordeling van de rechtmatigheid van de uitvoering van een bepaald gezichtsherkenningstechnologieproject; assisteren bij de uitvoering van de gegevensbeschermingseffectbeoordeling; waarborgen van de eerbiediging en uitoefening van de rechten van de betrokkenen.
- Proceseigenaar: optreden als de specifieke eenheid binnen de bevoegde rechtshandhavingsinstantie voor de ontwikkeling van het project die de details van het gezichtsherkenningstechnologieproject bepaalt, waaronder de vereisten voor de prestaties van het systeem; beslissen over de gepaste maatstaf voor billijkheid; vaststellen van de betrouwbaarheidsscore[71]; vaststellen van aanvaardbare drempels voor vooringenomenheid; vaststellen van de potentiële risico's van het gezichtsherkenningstechnologieproject voor de rechten en vrijheden van de individuen (door ook de DPO en de afdeling voor IT/AI en/of Gegevenswetenschap te raadplegen (zie hieronder) en deze risico's voor te leggen aan het hogere management. De proceseigenaar raadpleegt tevens de beheerder van de referentiedatabase alvorens te beslissen over de details van het gezichtsherkenningstechnologieproject, om inzicht te krijgen in zowel het gebruiksdoel als de technische details van de referentiedatabase. Wanneer ingekochte gezichtsherkenningstechnologie opnieuw moet worden getraind, is de proceseigenaar ook verantwoordelijk voor het kiezen van de trainingsdataset. Als de eenheid die is belast met het ontwikkelen en bepalen van de details van het project, is de proceseigenaar verantwoordelijk voor de uitvoering van de gegevensbeschermingseffectbeoordeling.
- Afdeling IT/AI en/of Gegevenswetenschap: assisteren bij het uitvoeren van een gegevensbeschermingseffectbeoordeling; uitleggen welke maatstaven beschikbaar zijn voor het meten van de systeemprestaties, billijkheid[72] en potentiële vooringenomenheid; implementeren van de technologie en de technische waarborgen, om ongeautoriseerde toegang tot de verzamelde gegevens, cyberaanvallen enz. te voorkomen. Wanneer ingekochte gezichtsherkenningstechnologie opnieuw getraind moet worden, traint de afdeling IT/AI of Gegevenswetenschap het systeem op basis van de door de proceseigenaar aangeleverde trainingsdataset. Deze afdeling is ook verantwoordelijk voor het treffen van maatregelen om de gezamenlijk door de proceseigenaren vastgestelde risico's te beperken (bijv. specifieke AI-risico's zoals deductieve aanvallen op het model).

[70] De volgende rollen zijn indicatief voor de verschillende belanghebbenden en hun verantwoordelijkheden in een gezichtsherkenningstechnologieproject. De rollen in deze bijlage worden beschreven in niet-assertieve bewoordingen en elke rechtshandhavingsinstantie dient op basis van haar organisatie vergelijkbare rollen vast te stellen en toe te wijzen. Het kan voorkomen dat een eenheid meerdere rollen op zich neemt, bijvoorbeeld proceseigenaar en beheerder van de referentiedatabase, of proceseigenaar en afdeling IT/AI en/of Gegevenswetenschap (als de eenheid van de proceseigenaar over alle benodigde technische kennis beschikt).

[71] De betrouwbaarheidsscore is het betrouwbaarheidsniveau van de voorspelling (match) in de vorm van een kansverwachting. Als er bijvoorbeeld twee templates worden vergeleken, is er een betrouwbaarheid van 90 % dat deze van dezelfde persoon zijn. De betrouwbaarheidsscore is niet hetzelfde als de prestaties van de gezichtsherkenningstechnologie, maar beïnvloedt deze wel. Hoe hoger de betrouwbaarheidsdrempel, hoe minder foutpositieven en hoe meer foutnegatieven in de resultaten van gezichtsherkenningstechnologie.

[72] Billijkheid kan worden gedefinieerd als het ontbreken van oneerlijke, onrechtmatige discriminatie, zoals vooroordelen op grond van geslacht of ras.

- Eindgebruikers (zoals politieagenten in het veld of in forensische laboratoria): een vergelijking met de database uitvoeren; kritisch beoordelen van de resultaten, rekening houdend met eerder bewijsmateriaal, en feedback geven aan de proceseigenaar bij foutpositieve resultaten en aanwijzingen van mogelijke discriminatie.
- Beheerder van de referentiedatabase: de specifieke eenheid binnen de bevoegde rechtshandhavingsinstantie die verantwoordelijk is voor het verzamelen en beheren van de referentiedatabase, d.w.z. de database waarmee de beelden worden vergeleken. Hieronder valt ook het verwijderen van gezichtsopnamen na de vastgestelde bewaartermijn. Een dergelijke database kan specifiek voor het beoogde gezichtsherkenningstechnologieproject worden aangemaakt of kan reeds bestaan voor verenigbare doeleinden. De beheerder van de referentiedatabase is verantwoordelijk voor het bepalen wanneer en onder welke omstandigheden gezichtsopnamen kunnen worden opgeslagen, alsook voor het vaststellen van de vereisten inzake gegevensbewaring (op grond van tijd of andere criteria).

Aangezien in de meeste gevallen waarin gezichtsherkenningstechnologie wordt ingezet en gebruikt, een inherent hoog risico voor de rechten en vrijheden van betrokkenen bestaat, moet in het kader van de op grond van artikel 28 RGR vereiste voorafgaande raadpleging ook de toezichthoudende autoriteit voor gegevensbescherming worden betrokken.

2. AANLOOP/VÓÓR DE AANKOOP VAN HET SYSTEEM VOOR GEZICHTSHERKENNINGSTECHNOLOGIE

De proceseigenaar in een rechtshandhavingsinstantie moet eerst een duidelijk begrip hebben van het proces of de processen die met het gebruik van de gezichtsherkenningstechnologie worden nagestreefd (de gebruikssituatie(s)) en moet waarborgen dat er een rechtsgrondslag is waarop de beoogde gebruikssituatie is gestoeld. Op basis hiervan moet de proceseigenaar:

- Formeel de gebruikssituatie beschrijven. Er moet worden beschreven welk probleem moet worden opgelost en op welke manier dit met gezichtsherkenningstechnologie kan worden opgelost. Ook moet een overzicht worden gegeven van het proces (de taak) waarin de technologie wordt toegepast. In dit verband moeten de rechtshandhavingsinstanties ten minste het volgende documenteren[73]:
  - de categorieën persoonsgegevens die in het proces worden vastgelegd;
  - de doelstellingen en concrete doeleinden waarvoor de gezichtsherkenningstechnologie wordt gebruikt, met inbegrip van de mogelijke gevolgen voor de betrokkene na een match;
  - wanneer en hoe de gezichtsopnamen worden verzameld (met inbegrip van informatie over de context van deze verzameling, bijv. bij de gate op de luchthaven, video's van beveiligingscamera's buiten een winkel waar een strafbaar feit is gepleegd enz. en de categorieën betrokkenen van wie de biometrische gegevens worden verwerkt);
  - de database waarmee de beelden worden vergeleken (referentiedatabase), evenals informatie over hoe deze is gemaakt, de omvang ervan en de kwaliteit van de biometrische gegevens die deze bevat;
  - de actoren die geautoriseerd worden om het gezichtsherkenningstechnologiesysteem te gebruiken en naar aanleiding hiervan te handelen in het kader van rechtshandhaving (hun profielen en toegangsrechten moeten worden opgegeven door de proceseigenaar);

[73] Bijlage I bevat een lijst van elementen die de verwerkingsverantwoordelijke kan gebruiken om een gebruikssituatie van gezichtsherkenningstechnologie te beschrijven.

- de beoogde bewaartermijn voor de ingevoerde gegevens, of het moment dat bepalend is voor het einde van deze termijn (zoals de afsluiting of beëindiging van de op grond van het nationale procesrecht gevoerde strafrechtelijke procedure waarvoor de gegevens oorspronkelijk zijn verzameld), evenals alle daaropvolgende acties (verwijdering van deze gegevens, anonimisering en gebruik voor statistische of onderzoeksdoeleinden enz.);
- implementatie van het logboek en de toegankelijkheid van logbestanden en bijgehouden gegevens;
- de prestatiemaatstaven (bijv. nauwkeurigheid, precisie, recall, F1-score) en de minimaal aanvaardbare drempelwaarde voor elke maatstaf[74];
- een schatting van het aantal mensen waarop de gezichtsherkenningstechnologie wordt toegepast en in welke periode of bij welke gelegenheid dit plaatsvindt.

- Een noodzakelijkheids- en evenredigheidsbeoordeling uitvoeren[75]. Het feit dat deze technologie bestaat, mag niet de drijfveer zijn om deze toe te passen. De proceseigenaar moet eerst beoordelen of er een passende rechtsgrondslag bestaat voor de beoogde verwerking. Hiervoor moeten de DPO en de juridische dienst worden geraadpleegd. De drijfveer om gezichtsherkenningstechnologie in te zetten moet zijn dat het een noodzakelijke en evenredige oplossing is voor een specifiek omschreven probleem van rechtshandhavingsinstanties. Dit moet worden beoordeeld op basis van het doel/de ernst van het strafbaar feit/het aantal personen dat niet is betrokken, maar wel gevolgen ondervindt van het gezichtsherkenningstechnologiesysteem. Voor de beoordeling van de rechtmatigheid moet ten minste het volgende in overweging worden genomen: RGR[76], AVG[77,78], elk bestaand rechtskader inzake AI[79] en alle bijbehorende richtsnoeren van toezichthoudende autoriteiten voor gegevensbescherming (zoals de Richtsnoeren 3/2019 inzake de verwerking van persoonsgegevens door middel van videoapparatuur[80] van de EDPB). Deze handelingen van

[74] Er zijn verschillende maatstaven om de prestaties van een gezichtsherkenningstechnologiesysteem te beoordelen. Elke maatstaf geeft een andere weergave van de systeemresultaten. In hoeverre deze erin slagen een adequaat beeld te geven van het al dan niet goed presteren van het systeem voor gezichtsherkenningstechnologie, is afhankelijk van de gebruikssituatie van deze technologie. Indien de nadruk ligt op een hoog percentage correct gekoppelde gezichten, kunnen maatstaven zoals precisie en recall worden gebruikt. Deze maatstaven meten echter niet hoe goed de gezichtsherkenningstechnologie omgaat met negatieve voorbeelden (hoeveel gezichten verkeerd werden gekoppeld door het systeem). De proceseigenaar moet, ondersteund door de afdelingen IT/AI en Gegevenswetenschap, in staat zijn om de vereisten voor prestaties te bepalen en deze uit te drukken in de meest geschikte maatstaf overeenkomstig de gebruikssituatie van de gezichtsherkenningstechnologie.

[75] Voor het noodzakelijkheidsbeginsel kunnen verdere stappen worden overwogen met betrekking tot de aanpassing en het gebruik van het systeem. De beschrijving van de gebruikssituatie kan dus ook enigszins worden gewijzigd tijdens de beoordeling op noodzakelijkheid en evenredigheid.

[76] Richtlijn 2016/680/EU van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

[77] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

[78] In gevallen waarin in een wetenschappelijk project voor onderzoek naar het gebruik van gezichtsherkenningstechnologie persoonsgegevens moeten worden verwerkt, maar die verwerking niet onder artikel 4, lid 3, RGR valt, zal in het algemeen de AVG van toepassing zijn (artikel 9, lid 2, RGR). In het geval van proefprojecten die worden gevolgd door rechtshandhavingsoperaties, blijft de RGR van toepassing.

[79] Er is bijvoorbeeld een voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op artificiële intelligentie) een tot wijziging van bepaalde wetgevingshandelingen van de Unie, maar dit voorstel is nog niet vastgesteld als verordening.

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

Unierecht moeten altijd stroken met de toepasselijke nationale voorschriften, met name op het gebied van het strafprocesrecht. In de evenredigheidsbeoordeling moet worden vastgesteld welke grondrechten van betrokkenen mogelijk worden aangetast (naast privacy en gegevensbescherming). Ook moeten hierin eventuele opgelegde beperkingen (of het ontbreken van beperkingen) in de gebruikssituatie van het systeem voor gezichtsherkenningstechnologie worden beschreven en nagegaan. Bijvoorbeeld of het systeem continu of tijdelijk actief is en of het beperkt wordt tot een geografisch gebied.

- Een gegevensbeschermingseffectbeoordeling uitvoeren[81]. Omdat de inzet van gezichtsherkenningstechnologie op het gebied van rechtshandhaving een hoog risico inhoudt voor de rechten en vrijheden van personen, moet een gegevensbeschermingseffectbeoordeling (PEB) worden uitgevoerd[82]. In het bijzonder bevat de PEB: een algemene beschrijving van de beoogde verwerkingsactiviteiten[83], een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen[84], de beoogde maatregelen ter beperking van deze risico's en de waarborgen, beveiligingsmaatregelen en mechanismen om ervoor te zorgen dat de persoonsgegevens worden beschermd en om aan te tonen dat de regelgeving wordt nageleefd. De PEB is een doorlopend proces, dus alle nieuwe elementen van de verwerking moeten worden toegevoegd en de risicobeoordeling moet in elke fase van het project worden bijgewerkt.
- Goedkeuring verkrijgen van het hogere management door toelichting van de risico's voor de rechten en vrijheden van betrokkenen (van de gebruikssituatie en de technologie) en de plannen om de respectieve risico's aan te pakken.

3. TIJDENS DE AANBESTEDING EN VÓÓR DE UITROL VAN DE GEZICHTSHERKENNINGSTECHNOLOGIE

- Criteria voor het kiezen van de gezichtsherkenningstechnologie (het algoritme) bepalen. De proceseigenaar moet de criteria voor het kiezen van een algoritme bepalen, met hulp van de afdeling IT/AI en/of Gegevenswetenschap. In de praktijk zouden de in de beschrijving van de gebruikssituatie vastgestelde maatstaven voor billijkheid en prestaties hier deel van uitmaken. Deze criteria moeten ook informatie bevatten over de gegevens waarmee het algoritme is getraind. De trainings-, test- en validatiesets moeten in voldoende mate monsters bevatten van alle kenmerken van de betrokkenen waarop de gezichtsherkenningstechnologie kan worden

[81] Nadere richtsnoeren over gegevensbeschermingseffectbeoordelingen zijn te vinden op: Richtsnoeren betreffende gegevensbeschermingseffectbeoordeling en om te bepalen of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening (EU) 2016/679, WP 248 rev.01, beschikbaar op: https://ec.europa.eu/newsroom/article29/items/611236 en de Engelstalige toolkit Accountability on the ground, part II, van de EDPS, beschikbaar op: https://edps.europa.eu/node/4582_en.

[82] Afhankelijk van de gebruikssituatie kan gezichtsherkenningstechnologie onder de volgende criteria vallen en verwerking met een hoog risico inhouden (uit de richtsnoeren betreffende gegevensbeschermingseffectbeoordeling, WP 248 rev. 01): systematische monitoring, gegevensverwerking op grote schaal, het matchen of combineren van datasets, innovatief gebruik of het toepassen van nieuwe technologische of organisatorische oplossingen.

[83] Zoals reeds beschreven in de bovenstaande stappen, maken de beschrijving van de verwerking en de beoordeling op noodzakelijkheid en evenredigheid ook deel uit van de gegevensbeschermingseffectbeoordeling, naast de risicobeoordeling. Indien nodig zal in de PEB een meer gedetailleerde beschrijving van de stromen van persoonsgegevens worden gegeven.

[84] In de risicoanalyse voor de betrokkenen moeten de risico's worden opgenomen die verband houden met de plaats van de te vergelijken gezichtsopnamen (lokaal/op afstand), de risico's in verband met verwerkers/subverwerkers en de risico's die specifiek zijn voor machinaal leren wanneer dit wordt toegepast (bijv. datavergiftiging, vijandige voorbeelden).

toegepast (denk bijvoorbeeld aan leeftijd, geslacht en ras) om vooringenomenheid te beperken. De aanbieder van de gezichtsherkenningstechnologie moet informatie en cijfers verstrekken over de trainings-, test- en validatiedatasets van de gezichtsherkenningstechnologie en moet een beschrijving geven van de maatregelen die zijn getroffen om mogelijke onrechtmatige discriminatie en vooringenomenheid te meten en te beperken. De proceseigenaar moet waar mogelijk nagaan of er een rechtsgrondslag bestond voor de aanbieder om deze dataset te gebruiken voor het trainen van de algoritmen (op basis van de door de aanbieder beschikbaar gestelde informatie). De proceseigenaar moet ervoor zorgen dat de aanbieder van de gezichtsherkenningstechnologie de beveiligingsnormen voor biometrische gegevens toepast, zoals ISO/IEC 24745, waarin richtsnoeren worden gegeven voor de bescherming van biometrische informatie krachtens diverse vereisten inzake vertrouwelijkheid, integriteit en hernieuwbaarheid/herroepbaarheid tijdens de opslag en doorgifte, alsook vereisten en richtsnoeren voor het veilig en conform de privacyregels beheren en verwerken van biometrische informatie.

- Het algoritme hertrainen (indien nodig). De proceseigenaar moet ervoor zorgen dat het afstemmen van het gezichtsherkenningstechnologiesysteem om een hogere nauwkeurigheid te bereiken voordat het wordt gebruikt, ook onderdeel uitmaakt van de ingekochte diensten. Wanneer aanvullende training van het verworven gezichtsherkenningstechnologiesysteem nodig is om aan de nauwkeurigheidscriteria te voldoen, moet de proceseigenaar, naast het nemen van de beslissing om het systeem te hertrainen, met hulp van de afdeling IT/AI en/of Gegevenswetenschap beslissen over de adequate, representatieve dataset die moet worden gebruikt en controleren of dit gebruik rechtmatig is voor de gegevens.
- De juiste waarborgen instellen om risico's met betrekking tot beveiliging, vooringenomenheid en slechte prestaties aan te pakken. Dit omvat het vaststellen van een proces om de gezichtsherkenningstechnologie te monitoren zodra deze in gebruik is (logbestanden en feedback voor de nauwkeurigheid en billijkheid van de resultaten). De proceseigenaar moet er daarnaast voor zorgen dat de specifieke risico's van sommige machinelearning- en gezichtsherkenningstechnologiesystemen (bijv. datavergiftiging, vijandige voorbeelden, modelinversie, whitebox-deductie) worden vastgesteld, gemeten en beperkt. De proceseigenaar moet ook passende waarborgen instellen om ervoor te zorgen dat de gegevensbewaringsvereisten voor de biometrische gegevens in de hertrainingsdataset worden nageleefd.
- Het gezichtsherkenningstechnologiesysteem documenteren. Dit omvat een algemene beschrijving van het systeem voor gezichtsherkenningstechnologie, een gedetailleerde beschrijving van de onderdelen van dit systeem en van het proces voor de totstandkoming ervan, gedetailleerde informatie over de bewaking, werking en bediening van het gezichtsherkenningstechnologiesysteem en een gedetailleerde beschrijving van de risico's en risicobeperkende maatregelen. In de onderdelen van deze documentatie worden belangrijke elementen van de beschrijving van het gezichtsherkenningstechnologiesysteem uit de eerdere fasen opgenomen (zie hierboven). Deze worden echter uitgebreid met informatie over het bewaken van de prestaties en het doorvoeren van veranderingen in het systeem, waaronder eventuele versiebijwerkingen en/of hertraining.
- Gebruikershandleidingen maken, met een uitleg van de technologie en de gebruikssituaties. In deze handleidingen moeten alle scenario's en voorwaarden voor het gebruik van gezichtsherkenningstechnologie op een duidelijke manier worden uitgelegd.
- De eindgebruikers opleiden in het gebruik van de technologie. In dergelijke trainingen moeten de mogelijkheden en beperkingen van de technologie worden uitgelegd, zodat de gebruikers begrijpen onder welke omstandigheden het nodig is om deze te gebruiken en in welke gevallen de technologie onnauwkeurig kan zijn. Deze trainingen zullen ook bijdragen aan het beperken van risico's in verband met het niet controleren of niet bekritiseren van de uitkomst van het algoritme.

- De toezichthoudende autoriteit voor gegevensbescherming raadplegen overeenkomstig artikel 28, lid 1, punt b), RGR. Informatie verstrekken volgens artikel 13 RGR om de betrokkenen te informeren over de verwerking en hun rechten. Deze kennisgevingen moeten in de juiste taal aan de betrokkenen worden gericht, zodat deze de verwerking kunnen begrijpen. Ook moeten de basiselementen van de technologie worden uitgelegd, waaronder nauwkeurigheidspercentages, trainingsdatasets en de getroffen maatregelen om discriminatie en een lage nauwkeurigheid van het algoritme te voorkomen.

4. AANBEVELINGEN NA HET INSTALLEREN VAN DE GEZICHTSHERKENNINGSTECHNOLOGIE

- Zorgen voor menselijke tussenkomst en menselijk toezicht op de resultaten. Er mag nooit een maatregel ten aanzien van een persoon worden genomen die uitsluitend is gebaseerd op het resultaat van de gezichtsherkenningstechnologie (dit zou een schending inhouden van artikel 11 RGR, geautomatiseerde individuele besluitvorming met juridische of andere soortgelijke gevolgen voor de betrokkene). Er moet worden gewaarborgd dat een medewerker van de rechtshandhavingsinstantie de resultaten van de gezichtsherkenningstechnologie evalueert. Tevens moet worden gewaarborgd dat de gebruikers van rechtshandhavingsinstanties de zogenoemde “automation bias” (vooringenomenheid in automatisering) vermijden, door tegenstrijdige informatie te onderzoeken en de resultaten van de technologie kritisch ter discussie te stellen. Hierbij is permanente opleiding en bewustmaking van de eindgebruikers belangrijk. Het hogere management moet er echter voor zorgen dat er voldoende personele middelen beschikbaar zijn om doeltreffend toezicht uit te oefenen. Dit houdt in dat elke agent voldoende tijd krijgt om de resultaten van de technologie kritisch ter discussie te stellen. Er moet worden vastgelegd, gemeten en beoordeeld in welke mate de oorspronkelijke beslissing van de gezichtsherkenningstechnologie verandert door menselijk toezicht.
- Volgen en aanpakken van de modeldrift van de gezichtsherkenningstechnologie (prestatieverslechtering) wanneer het model eenmaal in productie is.
- Een proces vaststellen voor de herbeoordeling van de risico’s en de beveiligingsmaatregelen, regelmatig en elke keer dat er wijzigingen worden aangebracht in de technologie of de gebruikssituatie.
- Elke wijziging in het systeem documenteren gedurende de hele levenscyclus (bijv. upgrades, hertraining).
- Een proces en de bijbehorende technische mogelijkheden vaststellen voor het behandelen van verzoeken om inzage van betrokkenen. De technische mogelijkheid om gegevens te extraheren, voor het geval deze aan de betrokkenen moeten worden verstrekt, moet beschikbaar zijn voordat een verzoek binnenkomt.
- De toepassing van procedures voor gegevensinbreuken waarborgen. Mocht er een inbreuk op persoonsgegevens plaatsvinden waarbij biometrische gegevens betrokken zijn, dan zijn de risico’s waarschijnlijk hoog. In dat geval moeten alle betrokken gebruikers op de hoogte zijn van de te volgen procedures, moet de functionaris voor gegevensbescherming onmiddellijk op de hoogte worden gebracht en moeten de betrokkenen worden geïnformeerd.

BIJLAGE III – PRAKTISCHE VOORBEELDEN

Er zijn veel verschillende praktische settings en doeleinden voor het gebruik van gezichtsherkenning, bijvoorbeeld in gecontroleerde omgevingen zoals bij grensovergangen, kruiscontroles met gegevens uit politiedatabases of op basis van persoonsgegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt, live camerabeelden (live gezichtsherkenning) enz. Bijgevolg variëren de risico's voor de bescherming van persoonsgegevens en andere rechten en vrijheden aanzienlijk in de verschillende gebruikssituaties. Om de beoordeling van de noodzakelijkheid en evenredigheid, die vooraf moet gaan aan de beslissing over de mogelijke inzet van gezichtsherkenning, te vergemakkelijken, geven de huidige richtsnoeren een niet-uitputtende lijst van mogelijke toepassingen van gezichtsherkenningstechnologie op het gebied van rechtshandhaving.

De gepresenteerde en beoordeelde scenario's zijn gebaseerd op **hypothetische** situaties en zijn bedoeld om bepaalde concrete toepassingen van gezichtsherkenningstechnologie te illustreren en hulp te bieden bij de overwegingen in elk geval, evenals een algemeen kader te schetsen. De lijst met scenario's pretendeert allerminst om uitputtend te zijn en laat onverlet alle lopende of toekomstige procedures van een nationale toezichthoudende autoriteit met betrekking tot het ontwerpen van, experimenteren met of toepassen van gezichtsherkenningstechnologieën. De presentatie van deze scenario's mag alleen dienen als voorbeeld van de reeds in dit document opgenomen richtsnoeren voor beleidsmakers, wetgevers en rechtshandhavingsinstanties bij het ontwerpen en uitwerken van de toepassing van gezichtsherkenningstechnologieën, teneinde volledige naleving van het EU-acquis op het gebied van de bescherming van persoonsgegevens te waarborgen. In dit verband mag niet uit het oog worden verloren dat zelfs in vergelijkbare situaties waarin gebruik wordt gemaakt van gezichtsherkenningstechnologie, de aanwezigheid of het ontbreken van bepaalde elementen kan leiden tot een andere uitkomst van de noodzakelijkheids- en evenredigheidsbeoordeling.

1 SCENARIO 1

1.1. Beschrijving

Een geautomatiseerd grenscontrolesysteem dat een geautomatiseerde grensovergang mogelijk maakt door de in het elektronische reisdocument opgeslagen biometrische afbeelding van EU-burgers en andere reizigers die de grensovergang passeren te authenticeren en vast te stellen dat de passagier de rechtmatige houder van het document is.

Bij deze verificatie/authenticatie is alleen sprake van één-op-ééngezichtsherkenning en uitvoering in een gecontroleerde omgeving (bijv. bij de e-gates op luchthavens). De biometrische gegevens van de reiziger die de grensovergang overgaat worden vastgelegd wanneer hij/zij expliciet wordt gevraagd om naar de camera in de e-gate te kijken en worden vergeleken met die van het voorgelegde document (paspoort, identiteitskaart enz.) dat volgens specifieke technische vereisten is afgegeven.

Hoewel de verwerking in dergelijke gevallen in beginsel buiten het toepassingsgebied van de richtlijn gegevensbescherming bij rechtshandhaving valt, kan de uitkomst van de verificatie tegelijkertijd ook worden gebruikt om de (alfanumerieke) gegevens van de persoon te vergelijken met rechtshandhavingsdatabases, als onderdeel van het grenstoezicht. Dit kan dus leiden tot acties met aanzienlijke rechtsgevolgen voor de betrokkene, bijvoorbeeld aanhouding op grond van een signalering in het SIS. Onder specifieke omstandigheden kunnen de biometrische gegevens ook worden gebruikt om te zoeken naar matches in rechtshandhavingsdatabases (in dat geval vindt in deze stap één-op-velenidentificatie plaats).

Het resultaat van de verwerking van het biometrische beeld heeft directe gevolgen voor de betrokkene: alleen als de verificatie succesvol is, kan hij of zij de grens overgaan. Wanneer het niet lukt de persoon te identificeren, moeten de grenswachten een tweede controle uitvoeren om na te gaan of de betrokkene iemand anders is dan de persoon in het identificatiedocument.

Wanneer een SIS- of nationale signalering wordt vastgesteld, moeten de grenswachten een tweede verificatie en de benodigde nadere controles uitvoeren en vervolgens de benodigde actie ondernemen, bijv. de persoon aanhouden of de betrokken autoriteiten op de hoogte brengen.

Bron van de informatie:
- Soorten betrokkenen: ☒ alle personen die de grenzen oversteken
- Bron van de afbeelding: ☒ overig (identiteitsdocument)
- Verband met strafbaar feit: ☒ niet noodzakelijk
- Wijze waarop de informatie wordt vastgelegd: ☒ in een cabine of in een gecontroleerde omgeving
- Context, gevolgen voor andere grondrechten: ja, te weten: ☒ recht op vrij verkeer ☒ recht op asiel

Referentiedatabase (waarmee de vastgelegde informatie wordt vergeleken):
- Specifiek karakter: ☒ specifieke databases voor grenscontrole

Algoritme:
- Soort verificatie: ☒ één-op-éénverificatie (authenticatie)

Resultaat:
- Effect ☒ direct (de betrokkene wordt de toegang verleend of geweigerd)
- Geautomatiseerde beslissing: ☒ ja

1.2. Toepasselijk rechtskader

Uit hoofde van Verordening (EG) nr. 2252/2004 van de Raad[85] moeten paspoorten en andere door de lidstaten afgegeven reisdocumenten sinds 2004 een biometrische gezichtsopname bevatten die is opgeslagen in een in het document ingesloten elektronische chip.

In de Schengengrenscode (SGC)[86] zijn de vereisten voor grenscontroles van personen aan de buitengrenzen bepaald. Voor EU-burgers en andere personen die krachtens het recht van de Unie het recht van vrij verkeer genieten, moeten de minimale controles bestaan uit een verificatie van hun reisdocumenten, in voorkomend geval door gebruik te maken van technische hulpmiddelen. De SGC is vervolgens gewijzigd bij Verordening (EU) 2017/2225[87], waarbij onder meer definities zijn ingevoerd voor “e-gates”, “geautomatiseerd grenscontrolesysteem” en “zelfbedieningssysteem”, alsmede de mogelijkheid om biometrische gegevens te verwerken voor het uitvoeren van grenscontroles.

Er mag dus worden aangenomen dat er een duidelijke en voorzienbare rechtsgrondslag bestaat op grond waarvan deze vorm van verwerking van persoonsgegevens is toegestaan. Bovendien is het rechtskader op het niveau van de Unie vastgesteld en rechtstreeks van toepassing op de lidstaten.

[85] Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten.
[86] Verordening (EU) 2016/399 van het Europees Parlement en de Raad van 9 maart 2016 betreffende een Uniecode voor de overschrijding van de grenzen door personen (Schengengrenscode).
[87] Verordening (EU) 2017/2225 van het Europees Parlement en de Raad van 30 november 2017 tot wijziging van Verordening (EU) 2016/399 in verband met het gebruik van het inreis-uitreissysteem.

1.3. Noodzaak en evenredigheid – doel/ernst van het strafbaar feit

De verificatie van de identiteit van EU-burgers via een geautomatiseerde grenscontrole aan de hand van hun biometrische afbeelding is een onderdeel van de grenscontroles aan de buitengrenzen van de EU. Bijgevolg houdt deze verificatie rechtstreeks verband met de beveiliging van de grenzen en dient deze een door de Unie erkende doelstelling van algemeen belang. Bovendien zorgen ABC-gates ervoor dat de passagiers sneller verwerkt kunnen worden en dat er minder risico is op menselijke fouten. Daarnaast is de reikwijdte, de omvang en de intensiteit van de inmenging in dit scenario veel beperkter dan bij andere vormen van gezichtsherkenning. Niettemin brengt de verwerking van biometrische gegevens extra risico's voor de betrokkenen met zich mee, die naar behoren moeten worden aangepakt en beperkt door de bevoegde autoriteit die de gezichtsherkenningstechnologie inzet en exploiteert.

1.4. Conclusie

De verificatie van de identiteit van EU-burgers in het kader van geautomatiseerd grenstoezicht is een noodzakelijke en evenredige maatregel zolang er passende waarborgen zijn ingesteld, met name de toepassing van de beginselen van doelbinding, gegevenskwaliteit, transparantie en een hoge mate van beveiliging.

2 SCENARIO 2

2.1. Beschrijving

Door de rechtshandhavingsinstanties wordt een systeem voor de identificatie van slachtoffers van kinderontvoering opgezet. Een bevoegde politiefunctionaris kan onder strikte voorwaarden de biometrische gegevens van een kind voor wie een vermoeden van ontvoering bestaat, vergelijken met een database van slachtoffers van kinderontvoering, uitsluitend om minderjarigen te identificeren die mogelijk overeenkomen met de beschrijving van het vermiste kind voor wie een onderzoek is ingesteld en de signalering is afgegeven.

Bij de verwerking in kwestie wordt het gezicht of de afbeelding van een persoon, die mogelijk overeenstemmen met de beschrijving van een vermist kind, vergeleken met de afbeeldingen in de database. Een dergelijke verwerking zou plaatsvinden in specifieke gevallen en niet op systematische basis.

De database waarmee de vergelijking wordt uitgevoerd, is gevuld met afbeeldingen van vermiste kinderen voor wie aangifte is gedaan van een vermoeden van kinderontvoering of een bedreigende situatie voor het leven of de fysieke integriteit van het kind, en voor wie uit hoofde van een gerechtelijke autoriteit een strafrechtelijk onderzoek is geopend en een signalering voor kinderontvoering is afgegeven. De gegevens worden verzameld in het kader van procedures die zijn vastgesteld door de bevoegde rechtshandhavingsautoriteit, dat wil zeggen politiefunctionarissen die gemachtigd zijn om justitiële politiemissies uit te voeren. De categorieën geregistreerde persoonsgegevens zijn:

- identiteit, bijnaam, alias, afstamming, nationaliteit, adressen, e-mailadressen, telefoonnummers;
- geboorteplaats en -datum;
- informatie over de afstamming;

- foto met technische kenmerken die het gebruik van een gezichtsherkenningsapparaat mogelijk maken en andere foto's.

De resultaten van de vergelijking moeten ook door een bevoegde functionaris worden beoordeeld en geverifieerd om eerdere bewijzen te staven met het resultaat van de vergelijking en eventuele foutpositieve resultaten uit te sluiten.

Foto's en persoonsgegevens van kinderen mogen alleen worden bewaard voor de duur van de signalering en moeten onmiddellijk na de afsluiting of beëindiging van de strafrechtelijke procedure worden gewist overeenkomstig de nationale procedures op grond waarvan deze in de database zijn ingevoerd.

Hoewel het mogelijk is om biometrische gegevens relatief lang in de database te bewaren en de bewaringstermijn overeenkomstig het nationale recht wordt vastgesteld, is voor de uitoefening van de rechten van de betrokkene en met name het recht op rectificatie en wissing voorzien in een aanvullende garantie om de inmenging in het recht op de bescherming van persoonsgegevens van de betrokkenen te beperken.

Bron van de informatie:
- Soorten betrokkenen: ☒ kinderen
- Bron van de afbeelding ☒ overig: niet vooraf gedefinieerd, vermoedelijk slachtoffer van kinderontvoering
- Verband met strafbaar feit ☒ niet direct temporeel ☒ niet direct geografisch
- Wijze waarop de informatie wordt vastgelegd: ☒ in een cabine of in een gecontroleerde omgeving
- Context: gevolgen voor andere grondrechten ☒ ja, te weten: ☒ verscheidene

Referentiedatabase (waarmee de vastgelegde informatie wordt vergeleken):
- Specifiek karakter ☒ specifieke database

Algoritme:
- Soort verificatie: ☒ één-op-velenidentificatie

Resultaat:
- Effect ☒ direct
- Geautomatiseerde beslissing: ☒ NEE, verplichte toetsing door een bevoegde functionaris

Juridische analyse:
- Toepasselijk rechtskader: ☒ specifieke nationale wetgeving voor deze verwerking (gezichtsherkenning)

2.2. Toepasselijk rechtskader

Het nationale recht voorziet in een specifiek rechtskader voor de database, waarin de doeleinden van de verwerking en de criteria voor het invullen, raadplegen en gebruiken van de database worden vastgesteld. De wetgevingsmaatregelen die nodig zijn voor de uitvoering ervan voorzien ook in de vaststelling van een bewaartermijn en verwijzen naar de toepasselijke beginselen van integriteit en vertrouwelijkheid. De wetgevingsmaatregelen voorzien ook in de modaliteiten voor de verstrekking van informatie aan de betrokkene en in dit geval de houder(s) van het ouderlijk gezag, evenals in de uitoefening van de rechten van de betrokkene en voor zover relevant de mogelijke beperking daarop. Tijdens de voorbereiding van het voorstel voor de respectieve wetgevingsmaatregel moest de nationale toezichthoudende autoriteit worden geraadpleegd.

2.3. Noodzakelijkheid en evenredigheid – doel/ernst van het strafbaar feit/aantal personen dat niet bij de verwerking is betrokken maar er wel door wordt getroffen

Voorwaarden en waarborgen voor de verwerking

De vergelijking via gezichtsherkenning kan alleen als laatste middel door een bevoegde ambtenaar worden uitgevoerd, wanneer er geen andere, minder ingrijpende middelen beschikbaar zijn en wanneer dat strikt noodzakelijk is, bijvoorbeeld in geval van twijfel over de authenticiteit van een identiteitsdocument van een reizende minderjarige en/of na onderzoek van eerder verzameld bewijsmateriaal en materiaal waaruit een mogelijke overeenstemming blijkt met de beschrijving van een vermist kind voor wie een strafrechtelijk onderzoek wordt uitgevoerd.

Er is ook voorzien in een aanvullende waarborg door de verplichte toetsing en verificatie van de vergelijking via gezichtsherkenning door een bevoegde functionaris, teneinde eerdere bewijzen te staven met het resultaat van de vergelijking en eventuele foutpositieve resultaten uit te sluiten.

Nagestreefde doelstelling

De oprichting van de database dient belangrijke doelstellingen van algemeen openbaar belang, met name de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen en de bescherming van de rechten en vrijheden van anderen. De oprichting van de database en de geplande verwerking lijken bij te dragen tot de identificatie van kinderen die het slachtoffer zijn van ontvoering en kunnen derhalve worden beschouwd als een maatregel die geschikt is ter ondersteuning van de legitieme doelstelling om dergelijke strafbare feiten te onderzoeken en te vervolgen.

Doeleinden en wijze van vullen van de database

De doeleinden van de verwerking zijn duidelijk bij wet vastgesteld en de database mag uitsluitend worden gebruikt voor het identificeren van vermiste kinderen voor wie aangifte is gedaan van een vermoeden van kinderontvoering, een strafrechtelijk onderzoek is ingesteld onder toezicht van een gerechtelijke autoriteit en een signalering voor de kinderontvoering is afgegeven. De in de wet bepaalde voorwaarden voor het vullen van de database zijn gericht op een strikte beperking van het aantal betrokkenen en persoonsgegevens die in de database worden opgenomen. De houder van het ouderlijk gezag over het kind moet worden geïnformeerd over de uitgevoerde verwerking en de voorwaarden voor de uitoefening van de rechten van het kind in verband met de beoogde biometrische verwerking voor identificatiedoeleinden of in verband met de in de database opgeslagen persoonsgegevens van het kind.

2.4. Conclusie

Gezien de noodzakelijkheid en evenredigheid van de beoogde verwerking, alsmede het belang van het kind bij de uitvoering van een dergelijke verwerking van persoonsgegevens, en op voorwaarde dat er voldoende waarborgen zijn om met name de uitoefening van de rechten van de betrokkene te garanderen – in het bijzonder gezien het feit dat er gegevens van kinderen worden verwerkt – kan een dergelijke toepassing van gezichtsherkenning als waarschijnlijk verenigbaar met het Unierecht worden beschouwd.

Gezien het soort verwerking en de gebruikte technologie, die een hoog risico voor de rechten en vrijheden van de betrokkene inhoudt, is de EDPB bovendien van mening dat de voorbereiding van een voorstel voor een door een nationaal parlement vast te stellen wetgevingsmaatregel of van een op

een dergelijke wetgevingsmaatregel gebaseerde regelgevingsmaatregel die verband houdt met de beoogde verwerking, een voorafgaande raadpleging van de toezichthoudende autoriteit moet omvatten om te zorgen voor consistentie en naleving van het toepasselijke rechtskader (zie artikel 28, lid 2, RGR).

3 SCENARIO 3

3.1. Beschrijving

In de loop van politie-interventies bij rellen en de daaropvolgende onderzoeken zijn een aantal personen als verdachten geïdentificeerd, bijv. in eerdere onderzoeken aan de hand van camerabeelden of getuigen. De foto's van deze verdachten worden vergeleken met foto's van personen die op de plaats delict of in de omliggende gebieden op CCTV of mobiele apparaten zijn opgenomen.

Om meer gedetailleerd bewijs te verkrijgen over personen die ervan worden verdacht te hebben deelgenomen aan rellen rond een demonstratie, maakt de politie een database die bestaat uit beeldmateriaal dat enigszins verband houdt met de plaats en het moment van de rellen. De database bevat door burgers naar de politie geüploade privé-opnamen, materiaal van CCTV-camera's in het openbaar vervoer, videobewakingsmateriaal van de politie en door de media gepubliceerd materiaal, zonder enige specifieke beperking of waarborg. Het vertonen van ernstig crimineel gedrag is geen voorwaarde voor het verzamelen van de bestanden in de database. Daardoor worden personen die niet bij de rellen betrokken waren – een aanzienlijk percentage van de lokale bevolking die toevallig langskwam op het moment van de demonstratie, of deelnam aan de demonstratie maar niet aan de rellen – opgeslagen in de database. Het gaat om duizenden video- en beeldbestanden.

Met behulp van gezichtsherkenningssoftware worden aan alle gezichten in die bestanden unieke gezichts-ID's toegekend. De gezichten van individuele verdachten worden vervolgens automatisch vergeleken met deze gezichts-ID's. De database met alle biometrische templates in de duizenden video- en beeldbestanden wordt opgeslagen totdat alle mogelijke onderzoeken zijn afgerond. Positieve matches worden behandeld door de verantwoordelijke agenten, die vervolgens beslissen over verdere maatregelen. Dit kan inhouden dat het in de database gevonden bestand wordt toegevoegd aan het strafdossier van de betreffende persoon. Ook kan het verdere maatregelen inhouden, zoals ondervraging of arrestatie van die persoon.

Een nationale wet voorziet in een algemene bepaling op grond waarvan het verwerken van biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon toelaatbaar is als dit strikt noodzakelijk is en behoudens passende waarborgen voor de rechten en vrijheden van de betrokkene.

Bron van de informatie:

- Soorten betrokkenen: ☒ alle personen
- Bron van de afbeelding: ☒ openbaar toegankelijke ruimten ☒ particuliere entiteit ☒ andere personen ☒ overig: media
- Verband met strafbaar feit: ☒ niet noodzakelijkerwijs een direct geografisch of temporeel verband
- Wijze van vastleggen van de informatie: ☒ op afstand
- Context, gevolgen voor andere grondrechten: ja, te weten ☒ de context van de vrijheid van vergadering
- Beschikbare aanvullende bronnen van informatie over de betrokkene:

☒ overig: niet uitgesloten (zoals het gebruik van geldautomaten of het binnengaan in een winkel), aangezien er geen controle kan worden uitgeoefend over de motieven op de foto's

Referentiedatabase (waarmee de vastgelegde informatie wordt vergeleken):

- Specifiek karakter: ☒ specifieke databases op misdaadgebied

Algoritme:

- Soort verwerking: ☒ één-op-velenidentificatie

Resultaat:

- Effect: ☒ direct (de betrokkene kan bijvoorbeeld worden gearresteerd of ondervraagd)
- Geautomatiseerde beslissing: ☒ NEE
- Duur van de opslag: totdat alle mogelijke onderzoeken zijn beëindigd

Juridische analyse:

- Soort voorafgaande informatie aan de betrokkene: ☒ op de website van de rechtshandhavingsinstantie in het algemeen
- Toepasselijk rechtskader: ☒ RGR grotendeels overgenomen in nationaal recht ☒ algemeen nationaal recht voor het gebruik van biometrische gegevens door rechtshandhavingsinstanties

3.2. Toepasselijk rechtskader

Zoals hierboven verduidelijkt, zijn rechtsgrondslagen die enkel de algemene bepaling van artikel 10 RGR herhalen, niet duidelijk genoeg in hun bewoordingen om individuen een adequate indicatie te geven van de voorwaarden waaronder en de omstandigheden waarin rechtshandhavingsinstanties gemachtigd zijn om CCTV-opnames uit openbare ruimten te gebruiken voor het creëren van een biometrische template van hun gezicht en dit te vergelijken met politiedatabases, andere beschikbare CCTV- of privé-opnames enz. Het in dit scenario vastgestelde rechtskader voldoet daarom niet aan de minimumvereisten om als rechtsgrondslag te dienen.

3.3. Noodzakelijkheid en evenredigheid

In dit voorbeeld geeft de verwerking om verschillende redenen aanleiding tot bezorgdheid in het kader van het noodzakelijkheids- en het evenredigheidsbeginsel:

De personen worden niet verdacht van een ernstig strafbaar feit. Het vertonen van ernstig crimineel gedrag is geen voorwaarde voor het gebruik van de bestanden in de database die het beeldmateriaal bevat. Bovendien is een rechtstreeks temporeel en geografisch verband met het strafbare feit geen voorwaarde voor het gebruik van de bestanden in de database. Hierdoor wordt een aanzienlijk percentage van de lokale bevolking mogelijk meerdere jaren lang in een biometrische database opgeslagen, totdat alle onderzoeken worden beëindigd.

De database van de plaats delict is niet beperkt tot beelden die voldoen aan de vereisten voor evenredigheid, waardoor een onbeperkt aantal beelden kan worden vergeleken. Dit is in strijd met het beginsel van gegevensminimalisatie. Bij een kleinere hoeveelheid afbeeldingen zouden ook niet-

algoritmische en minder ingrijpende middelen in overweging kunnen worden genomen, zoals superherkenners[88].

Aangezien het voorbeeld betrekking heeft op de omgeving van een demonstratie, is het ook waarschijnlijk dat uit de beelden de politieke opvattingen van de deelnemers aan de demonstratie duidelijk worden, de tweede speciale categorie gegevens waarvoor dit scenario mogelijk ongunstige gevolgen heeft. In dit scenario is het onduidelijk hoe het verzamelen van deze gegevens kan worden voorkomen en met welke waarborgen. Wanneer betrokkenen te weten komen dat hun deelname aan een demonstratie heeft geleid tot opname in een biometrische politiedatabase, kan dit bovendien ernstige afschrikkende effecten hebben voor de toekomstige uitoefening van hun recht op vergadering.

De biometrische templates in de database kunnen ook met elkaar worden vergeleken. Hierdoor kan de politie niet alleen in al haar materiaal naar een specifieke persoon zoeken, maar ook het gedragspatroon van een persoon in de loop van een aantal dagen reconstrueren. De politie kan ook aanvullende informatie over de personen verzamelen, zoals sociale contacten en politieke betrokkenheid.

De inmenging wordt verder versterkt door het feit dat de gegevens worden verwerkt zonder dat de betrokkenen hiervan op de hoogte zijn.

Gezien het feit dat mensen voortdurend foto's maken en video's opnemen en dat zelfs de alomtegenwoordige CCTV-opnamen biometrisch kunnen worden geanalyseerd, kan dit leiden tot ernstige afschrikkende effecten.

Het wijdverbreide gebruik van privéfoto's en video's, met inbegrip van mogelijk misbruik zoals iemand verklikken, is een ander punt van zorg. Gezien het feit dat misbruik zoals het verklikken van een persoon een risico is dat ook inherent is aan strafrechtelijke procedures in het algemeen, is het risico aanzienlijk hoger naargelang de schaalbaarheid van de verwerkte gegevens en het aantal betrokken personen. Mensen kunnen immers ook materiaal uploaden dat betrekking heeft op een specifieke persoon of een groep personen die hun niet aanstaat. Verzoeken van de politie om foto's en video's te uploaden leiden mogelijk tot zeer lage drempels voor mensen om materiaal te verstrekken, met name omdat het mogelijk is om dit anoniem te doen of ten minste zonder de noodzaak om zich op een politiebureau te presenteren en te identificeren.

3.4. Conclusie

In het voorbeeld is er geen sprake van een specifieke bepaling die als rechtsgrondslag zou kunnen dienen. Zelfs als er een toereikende rechtsgrondslag zou zijn, zou niet worden voldaan aan de vereisten van noodzakelijkheid en evenredigheid, wat zou leiden tot een onevenredige inmenging in het recht van de betrokkene op eerbiediging van het privéleven en de bescherming van persoonsgegevens uit hoofde van het Handvest.

[88] D.w.z. mensen met een buitengewoon vermogen om gezichten te herkennen. Zie ook: Face Recognition by Metropolitan Police Super-Recognisers, 2016 Feb 26, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

4 SCENARIO 4

4.1. Beschrijving

De politie past een manier toe voor de identificatie van verdachten die een ernstig strafbaar feit plegen dat op CCTV is vastgelegd, door met terugwerkende kracht gezichtsherkenningstechnologie te gebruiken. Een agent selecteert handmatig afbeelding(en) van verdachten in het videomateriaal dat in het kader van een vooronderzoek is verzameld op de plaats delict of elders en stuurt deze afbeelding(en) vervolgens naar de forensische afdeling. De forensische afdeling gebruikt gezichtsherkenningstechnologie om deze afbeelding(en) te vergelijken met foto's van personen die eerder door de politie in een database zijn verzameld (een zogenoemde beschrijvende database die bestaat uit verdachten en eerder veroordeelden). Bij deze procedure wordt de beschrijvende database – tijdelijk en in een geïsoleerde omgeving – geanalyseerd met gezichtsherkenningstechnologie om de vergelijking te kunnen uitvoeren. Om de inmenging in de rechten en belangen van de gekoppelde personen tot een minimum te beperken, heeft een zeer beperkt aantal medewerkers van de forensische afdeling toestemming om de feitelijke vergelijking uit te voeren, is de toegang tot de gegevens beperkt tot de functionarissen die belast zijn met het specifieke dossier en wordt een handmatige controle van de resultaten uitgevoerd voordat de resultaten aan de opsporingsfunctionaris worden toegezonden. De biometrische gegevens worden niet doorgegeven buiten de gecontroleerde, geïsoleerde omgeving. Alleen het resultaat en de foto (niet de biometrische template) worden verder gebruikt in het onderzoek. De medewerkers krijgen specifieke training over de regels en procedures voor deze verwerking en alle verwerkingen van persoonlijke en biometrische gegevens zijn voldoende gespecificeerd in de nationale wetgeving.

Bron van de informatie:

- Soorten betrokkenen: ☒ verdachten die zijn geïdentificeerd aan de hand van de CCTV-opnamen
- Bron van de afbeelding: ☒ openbaar toegankelijke ruimten ☒ internet
- Verband met strafbaar feit: ☒ direct temporeel
  ☒ direct geografisch
- Wijze van vastleggen van de informatie: ☒ op afstand
- Context, gevolgen voor andere grondrechten: ja, te weten: ☒ vrijheid van vergadering ☒ vrijheid van meningsuiting ☒ verscheidene: __

Referentiedatabase (waarmee de vastgelegde informatie wordt vergeleken):

- Specifiek karakter: ☒ specifieke databases op misdaadgebied

Algoritme:

- Soort verwerking: ☒ één-op-velenidentificatie

Resultaat:

- Effect: ☒ direct (bijv. de betrokkene wordt gearresteerd of ondervraagd)
- Geautomatiseerde beslissing: ☒ NEE

Juridische analyse:

- Toepasselijk rechtskader: ☒ bijzondere nationale wetgeving voor deze verwerking (gezichtsherkenning) voor de betreffende bevoegde autoriteit

4.2. Toepasselijk rechtskader

In dit scenario bepaalt de nationale wetgeving dat bij de uitvoering van forensische analyse biometrische gegevens mogen worden gebruikt wanneer dit strikt noodzakelijk is om verdachten die een ernstig strafbaar feit plegen, te identificeren door de foto's te vergelijken met de beschrijvende database. In de nationale wetgeving is bepaald welke gegevens mogen worden verwerkt en wat de procedures voor het bewaren van de integriteit en vertrouwelijkheid van persoonsgegevens en de procedures voor de vernietiging van de gegevens zijn, waardoor voldoende garanties worden geboden tegen het risico van misbruik en willekeur.

4.3. Noodzakelijkheid en evenredigheid

Op forensisch niveau is het gebruik van gezichtsherkenning duidelijk efficiënter qua tijd dan handmatige vergelijking. Door de handmatige selectie van afbeeldingen vooraf is de inmenging beperkter dan bij een vergelijking van al het videomateriaal met een database. Hierbij wordt een onderscheid tussen personen gemaakt en is de vergelijking alleen gericht op de personen die onder het doel vallen, d.w.z. het bestrijden van ernstige strafbare feiten. Het blijft echter belangrijk om na te gaan of de vergelijking, afhankelijk van het geval, binnen een redelijke termijn handmatig kan worden uitgevoerd. De gevolgen voor het recht op privacy en gegevensbescherming worden beperkt doordat het aantal personen met toegang tot de technologie en de persoonsgegevens beperkt is en de biometrische templates niet worden opgeslagen of later in het onderzoek worden gebruikt. De handmatige controle van het resultaat betekent ook een verminderd risico op foutpositieven.

4.4. Conclusie

Het is belangrijk dat de nationale wetgeving voorziet in een adequate rechtsgrondslag voor de verwerking van biometrische gegevens en voor de nationale database waarmee de gegevens worden vergeleken. In dit scenario zijn verschillende maatregelen getroffen om de inmenging in gegevensbeschermingsrechten te beperken, zoals de in de rechtsgrondslag bepaalde voorwaarden voor het gebruik van de gezichtsherkenningstechnologie, het aantal mensen dat toegang heeft tot de technologie en de biometrische gegevens, handmatige controles enz. De gezichtsherkenningstechnologie verbetert de efficiëntie van het onderzoekswerk van de forensische afdeling van de politie aanzienlijk, is gebaseerd op wetgeving die de politie toestaat biometrische gegevens te verwerken wanneer dat absoluut noodzakelijk is en kan daarom, binnen deze grenzen, worden beschouwd als een rechtmatige inmenging in de rechten van de persoon.

5 SCENARIO 5

5.1. Beschrijving

Biometrische identificatie op afstand vindt plaats wanneer de identiteit van personen met behulp van biometrische kenmerken (fysieke afbeelding, manier van lopen, iris enz.) op afstand, in een openbare ruimte en doorlopend of voortdurend wordt vastgesteld door de kenmerken te toetsen aan (biometrische) gegevens die in een database zijn opgeslagen[89]. Biometrische identificatie op afstand wordt in real time uitgevoerd indien de vastlegging van het beeldmateriaal, de vergelijking en de identificatie plaatsvinden zonder noemenswaardige vertraging.

Voorafgaand aan elke inzet in real time van biometrische identificatie op afstand stelt de politie een volglijst op van personen die in het kader van een onderzoek van belang zijn. Deze lijst wordt gevuld met gezichtsopnames van de individuele personen. Op basis van inlichtingen die suggereren dat de

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

individuen zich in een specifiek gebied zullen bevinden, zoals in een winkelcentrum of op een openbaar plein, beslist de politie wanneer, waar en hoe lang de biometrische identificatie op afstand wordt ingezet.

Op de dag van de actie zetten ze op die plaats een politiebusje neer als controlecentrum, met een senior politieagent aan boord. In het busje zijn monitoren aanwezig met beelden van in de buurt geplaatste CCTV-camera's die op ad-hocbasis zijn geïnstalleerd of waarbij verbinding wordt gemaakt met de videostreams van reeds geïnstalleerde camera's. Als voetgangers langs de camera's lopen, isoleert de technologie gezichtsopnamen, zet deze om in een biometrische template en vergelijkt deze met de biometrische templates van de personen op de volglijst.

Als een potentiële match wordt gedetecteerd tussen de volglijst en degenen die langs de camera's lopen, wordt er een waarschuwing gestuurd naar de agenten in het busje, die vervolgens de agenten ter plaatse adviseren als de waarschuwing positief is, bijvoorbeeld via een radio. De agent ter plaatse beslist vervolgens of hij of zij ingrijpt, de persoon benadert of deze uiteindelijk aanhoudt. De door de agent ter plaatse genomen maatregelen worden vastgelegd. In het geval van een discrete controle wordt de verzamelde informatie (zoals met wie de persoon is, wat ze dragen en waar ze naartoe gaan) opgeslagen.

Een nationale wet waarnaar wordt verwezen voorziet in een algemene bepaling volgens welke de verwerking van biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon toelaatbaar is indien dit strikt noodzakelijk is en onder voorbehoud van passende waarborgen voor de rechten en vrijheden van de betrokkene.

Bron van de informatie:

- Soorten betrokkenen: ☒ alle personen
- Bron van de afbeelding: ☒ openbaar toegankelijke ruimten
- Verband met strafbaar feit: ☒ niet noodzakelijkerwijs een direct geografisch of temporeel verband
- Wijze van vastleggen van de informatie: ☒ op afstand
- Context, gevolgen voor andere grondrechten: ja, te weten: ☒ vrijheid van vergadering ☒ vrijheid van meningsuiting ☒ verscheidene
- Beschikbare aanvullende bronnen van informatie over de betrokkene:
  ☒ overige: niet uitgesloten (zoals gebruik van geldautomaten of het binnengaan van winkels)

Referentiedatabase (waarmee de vastgelegde informatie wordt vergeleken):

- Specifiek karakter: ☒ specifieke databases op misdaadgebied

Algoritme:

- Soort verwerking: ☒ één-op-velenidentificatie

Resultaat:

- Effect: ☒ direct (de betrokkene wordt bijvoorbeeld gearresteerd of ondervraagd)
- Geautomatiseerde beslissing: ☒ NEE
- Duur van de opslag: totdat alle mogelijke onderzoeken zijn beëindigd

Juridische analyse:

- Soort voorafgaande informatie aan de betrokkene: ☒ op de website van de rechtshandhavingsinstantie in het algemeen

- Toepasselijk rechtskader: ☒ RGR grotendeels gekopieerd naar nationaal recht ☒ algemeen nationaal recht voor het gebruik van biometrische gegevens door rechtshandhavingsinstanties

5.2. Toepasselijk rechtskader

Zoals hierboven verduidelijkt, zijn rechtsgrondslagen die enkel de algemene bepaling van artikel 10 RGR herhalen, niet duidelijk genoeg in hun bewoordingen om individuen een adequate indicatie te geven van de voorwaarden waaronder en de omstandigheden waarin rechtshandhavingsinstanties gemachtigd zijn om CCTV-opnames uit openbare ruimten te gebruiken voor het creëren van een biometrisch template van hun gezicht en deze te vergelijken met politiedatabases. Het wettelijk kader dat in dit scenario is vastgesteld, voldoet dus niet aan de minimumvereisten om als rechtsgrondslag te dienen[90].

5.3. Noodzakelijkheid en evenredigheid

De lat voor noodzakelijkheid en evenredigheid wordt hoger naarmate de inmenging verder gaat. Biometrische identificatie op afstand in openbare ruimten heeft verschillende implicaties voor de grondrechten:

De scenario's hebben betrekking op het toezicht op alle voorbijgangers in de respectieve openbare ruimte. Er is dus sprake van een ernstige invloed op de redelijke verwachting van de bevolking om anoniem te zijn in openbare ruimten[91]. Dit is een voorwaarde voor veel facetten van het democratische proces, zoals de beslissing om lid te worden van een burgervereniging, bijeenkomsten te bezoeken en mensen van alle sociale en culturele achtergronden te ontmoeten, deel te nemen aan een politiek protest en allerlei soorten plaatsen te bezoeken. De notie van anonimiteit in openbare ruimtes is essentieel om vrijelijk informatie te verzamelen en ideeën op te doen en deze uit te wisselen. Zij beschermt de pluraliteit van meningen, de vrijheid van vreedzame vergadering en vereniging en de bescherming van minderheden en ondersteunt de beginselen van de scheiding der machten en teugels en tegenwichten. Het ondermijnen van de notie van anonimiteit in de openbare ruimte kan resulteren in een ernstig afschrikkend effect op burgers. Ze kunnen afzien van bepaalde gedragingen die binnen de grenzen van een vrije en open samenleving vallen. Dit zou gevolgen hebben voor het algemeen belang, aangezien in een democratische samenleving zelfbeschikking en deelname van haar burgers aan het democratische proces zijn vereist.

Als een dergelijke technologie wordt toegepast, zal het simpelweg lopen op straat, naar de metro of naar de bakker in het getroffen gebied leiden tot het verzamelen van persoonsgegevens, waaronder biometrische gegevens, door wetshandhavingsinstanties en in het eerste scenario ook tot vergelijking met politiedatabases. Een situatie waarin hetzelfde zou worden gedaan door vingerafdrukken te nemen, zou duidelijk onevenredig zijn.

Het aantal betrokkenen is buitensporig hoog, omdat iedereen die in de betreffende openbare ruimte voorbijloopt, wordt getroffen. Verder impliceren de scenario's een geautomatiseerde massale

[90] In gevallen waarin in een wetenschappelijk project voor onderzoek naar het gebruik van gezichtsherkenningstechnologie persoonsgegevens moeten worden verwerkt, maar die verwerking niet onder artikel 4, lid 3, RGR valt, zal de AVG van toepassing zijn. In het geval van proefprojecten die worden gevolgd door rechtshandhavingsoperaties, blijft de RGR van toepassing.

[91] Antwoord van de EDPB aan leden van het Europees Parlement met betrekking tot de door Clearview AI ontwikkelde applicatie voor gezichtsherkenning van 10 juni 2020, ref: OUT2020-0052.

verwerking van biometrische gegevens en ook een massale vergelijking van biometrische gegevens met politiedatabases.

In de hele Europese jurisprudentie is massasurveillance verboden (zo beschouwde het EHRM in S. en Marper tegen VK de ongedifferentieerde bewaring van biometrische gegevens als een "onevenredige inmenging" in het recht op privacy, aangezien die niet als "noodzakelijk in een democratische samenleving" wordt beschouwd).

Bij biometrische identificatie op afstand is de kans op massasurveillance zo groot dat er geen betrouwbare middelen tot beperking zijn. Het is wezenlijk verschillend van de reguliere videobewaking. Het mogelijke gebruik van videobeelden zonder biometrische identificatie is immers al een sterke, hoewel tegelijkertijd beperkte inmenging, maar als gezichtsherkenningstechnologie wordt toegepast, zal de aard van het reeds wijdverbreide videobewakingssysteem als belangrijkste bron van de gegevens een verandering ondergaan. Bovendien en met name met betrekking tot de impliciete afschrikkende effecten, zullen mogelijke beperkingen in de toepassing van het reeds bestaande videobewakingsnetwerk niet zichtbaar zijn en dus niet door het publiek worden vertrouwd.

Bij biometrische identificatie op afstand door politieautoriteiten wordt iedereen als een potentiële verdachte behandeld. In een rechtsstaat wordt er echter van uitgegaan dat burgers rechten hebben totdat wangedrag kan worden aangetoond. Dit beginsel komt ook gedeeltelijk tot uiting in de richtlijn gegevensbescherming bij rechtshandhaving, waarin wordt benadrukt dat er, voor zover mogelijk, een onderscheid moet worden gemaakt tussen de behandeling van veroordeelden of verdachten van strafbare feiten, in welk geval de rechtshandhavingsinstanties moeten beschikken over "*gegronde vermoedens [...] dat zij een strafbaar feit hebben gepleegd of zullen plegen*" (artikel 6, punt a), RGR) en personen die niet zijn veroordeeld of worden verdacht van strafbare activiteiten.

Bij toepassing op vervoersknooppunten of in openbare ruimten, waarbij rechtshandhavingsinstanties een technologie gebruiken die in staat is om een enkele persoon uniek te identificeren en zijn of haar verblijfplaats en bewegingen te traceren en analyseren, wordt in het ergste geval de meest gevoelige informatie over een persoon onthuld (zelfs seksuele voorkeuren, religie, gezondheidsproblemen). Dit gaat gepaard met het enorme risico van onrechtmatige toegang tot en gebruik van de gegevens.

De installatie van een systeem waarmee de kern van het gedrag en de persoonskenmerken van een individu kan worden blootgelegd, leidt tot sterke afschrikkende effecten. Mensen gaan zich afvragen of ze willen deelnemen aan een bepaalde manifestatie, wat schadelijk is voor het democratisch proces. Ook het in het openbaar ontmoeten en gezien worden met een bepaalde vriend die bekend staat als iemand die problemen heeft met de politie of zich op een unieke manier gedraagt, kan als hachelijk worden gezien, omdat dit alles zou leiden tot het aantrekken van het algoritme van het systeem en dus van rechtshandhaving.

Het is onmogelijk om kwetsbare betrokkenen zoals kinderen te beschermen. Daarnaast worden personen getroffen die er beroepsmatig belang bij hebben, vaak op grond van een wettelijke verplichting, om hun contacten vertrouwelijk te houden, zoals journalisten, advocaten en geestelijken. Dit kan bijvoorbeeld leiden tot de onthulling van de bron en de journalist, of van het feit dat een persoon een strafrechtadvocaat raadpleegt. Het probleem geldt niet alleen voor willekeurige openbare plaatsen, bijvoorbeeld waar journalisten en hun bronnen elkaar ontmoeten, maar ook voor openbare ruimten waar mensen naartoe moeten om instellingen of professionals op dit gebied te benaderen en er toegang toe te krijgen.

Bovendien kan het ongemak met gezichtsherkenningstechnologie ertoe leiden dat mensen hun gedrag veranderen door plaatsen waar gezichtsherkenningstechnologie wordt gebruikt te vermijden en zich

dus terug te trekken uit het sociale leven en culturele evenementen. Afhankelijk van de omvang van de inzet van de gezichtsherkenningstechnologie kan het effect op mensen zo groot zijn dat hun vermogen om een waardig leven te leiden wordt aangetast[92].

Daarom is er een grote kans dat de wezenlijke inhoud – de onaantastbare kern – van het recht op bescherming van persoonsgegevens wordt aangetast. Sterke aanwijzingen (zie punt 3.1.3.2 van de richtsnoeren) zijn met name de volgende: op grote schaal worden de unieke biologische kenmerken van mensen automatisch verwerkt door rechtshandhavingsinstanties, met algoritmen die gebaseerd zijn op aannemelijkheid met slechts een beperkte verklaarbaarheid van de resultaten. De beperkingen op het recht op privacy en op gegevensbescherming worden opgelegd ongeacht het individuele gedrag van de persoon of de omstandigheden die hem of haar betreffen. Statistisch gezien zijn bijna alle betrokkenen die door deze inmenging worden getroffen, personen die zich aan de wet houden. Er zijn slechts beperkte mogelijkheden om informatie aan de betrokkene te verstrekken. In de meeste gevallen zal pas in een later stadium beroep bij de rechter mogelijk zijn.

Het vertrouwen op een op aannemelijkheid gebaseerd systeem met een beperkte verklaarbaarheid kan leiden tot het spreiden van aansprakelijkheid en een gebrek aan rechtsmiddelen en kan mogelijk een stimulans vormen voor nalatigheid.

Zodra een dergelijk systeem, dat ook kan worden gebruikt voor bestaande CCTV-camera's, met weinig moeite en zonder zichtbaar te zijn voor de betrokkenen wordt toegepast, kan het worden misbruikt en worden ingeschakeld om systematisch en snel lijsten van personen op te stellen op basis van etnische afkomst, geslacht, godsdienst enz. Het beginsel van de verwerking van persoonsgegevens op basis van vooraf bepaalde criteria, zoals de verblijfplaats van een persoon en de afgelegde weg, wordt reeds toegepast[93] en is vatbaar voor discriminatie.

In overeenstemming met de gevoeligheid, de expressiviteit en de hoeveelheid verwerkte gegevens zijn systemen voor gezichtsherkenning op afstand op openbaar toegankelijke plaatsen vatbaar voor misbruik, met nadelige gevolgen voor de betrokken personen. Dergelijke gegevens kunnen ook gemakkelijk worden verzameld en misbruikt om de belangrijkste actoren in het beginsel van teugels en tegenwichten, zoals de politieke oppositie, agenten en journalisten, onder druk te zetten.

Tot slot bevatten systemen voor gezichtsherkenningstechnologie vaak sterke vooroordelen met betrekking tot ras en geslacht: foutpositieve resultaten treffen mensen van kleur en vrouwen onevenredig zwaar[94], wat leidt tot discriminatie. Politiemaatregelen na een foutpositief resultaat, zoals huiszoekingen en arrestaties, stigmatiseren deze groepen nog meer.

5.4. Conclusie

In de bovengenoemde scenario's voor verwerking op afstand van biometrische gegevens in openbare ruimten voor identificatiedoeleinden, is er geen sprake van een billijk evenwicht tussen de

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

[93] Zie artikel 6 van Richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit en artikel 33 van Verordening (EU) 2018/1240 van het Europees Parlement en de Raad van 12 september 2018 tot oprichting van een Europees reisinformatie- en -autorisatiesysteem (Etias) en tot wijziging van de Verordeningen (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 en (EU) 2017/2226.

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

concurrerende particuliere en openbare belangen, waardoor ze een onevenredige inmenging vormen op de rechten van de betrokkene uit hoofde van de artikelen 7 en 8 van het Handvest.

6 SCENARIO 6

6.1. Beschrijving

Een particuliere entiteit levert een applicatie waarbij via "scraping" gezichtsopnamen van het internet worden gehaald om een database aan te leggen. De gebruiker, bijvoorbeeld de politie, kan een foto uploaden en vervolgens zal de applicatie met behulp van biometrische identificatie proberen deze te vergelijken met de gezichtsopnamen of biometrische templates in de database.

Een lokale politieafdeling voert een onderzoek uit naar een op video opgenomen strafbaar feit waarbij een aantal mogelijke getuigen en verdachten niet kunnen worden geïdentificeerd via vergelijking van de verzamelde informatie met interne databases of inlichtingen. De betrokkenen zijn op basis van de verzamelde informatie niet geregistreerd in een bestaande politiedatabase. De politie besluit om een instrument te gebruiken zoals hierboven beschreven, dat wordt geleverd door een particulier bedrijf, om de personen te identificeren door middel van biometrische identificatie.

Bron van de informatie:

- Soorten betrokkenen: ☒ alle burgers (getuigen) ☒ veroordeelden ☒ verdachten
- Bron van de afbeelding: ☒ videobeelden van een openbare plaats of elders verzameld in het kader van een vooronderzoek
- Verband met strafbaar feit: ☒ niet noodzakelijk
- Wijze van vastleggen van de informatie: ☒ op afstand
- Context, gevolgen voor andere grondrechten: Ja, te weten: ☒ vrijheid van vergadering ☒ vrijheid van meningsuiting ☒ verscheidene: __

Referentiedatabase (waarmee de vastgelegde informatie wordt vergeleken):

- Specifiek karakter: ☒ databases voor algemeen gebruik die via internet zijn gevuld

Algoritme:

- Soort verwerking: ☒ één-op-velenidentificatie

Resultaat:

- Effect ☒ direct (bijv. de betrokkene wordt gearresteerd, ondervraagd, discriminerend gedrag)
- Geautomatiseerde beslissing: ☒ NEE

Juridische analyse:

- Soort voorafgaande informatie aan de betrokkene: ☒ nee

6.2. Toepasselijk rechtskader

Wanneer een private entiteit een dienst levert waarbij persoonsgegevens worden verwerkt waarvoor zij het doel en de middelen bepalen (in dit geval het "scrapen" van afbeeldingen van het internet om een database te maken), moet deze private entiteit beschikken over een rechtsgrondslag voor deze verwerking. Bovendien moet de rechtshandhavingsinstantie die besluit deze dienst voor haar doeleinden te gebruiken, over een rechtsgrondslag beschikken voor de verwerking waarvoor zij de doeleinden en middelen bepalen. Als de rechtshandhavingsinstantie de biometrische gegevens wil

kunnen verwerken, moet er een rechtskader zijn dat het doel, de te verwerken persoonsgegevens, de doeleinden van de verwerking en de procedures voor het bewaren van de integriteit en vertrouwelijkheid van de persoonsgegevens en de procedures voor de vernietiging ervan specificeert.

Dit scenario houdt in dat er op grote schaal persoonsgegevens worden verzameld van personen die zich er niet van bewust zijn dat hun gegevens worden verzameld. Een dergelijke verwerking kan slechts in zeer uitzonderlijke omstandigheden rechtmatig zijn. Afhankelijk van waar de database zich bevindt, kan het gebruik van een dergelijke dienst inhouden dat persoonsgegevens en/of bijzondere categorieën persoonsgegevens buiten de Europese Unie worden doorgegeven (door de politie, bijvoorbeeld door het "verzenden" van de gezichtsopname in de observatievideo of een op een andere manier verzamelde opname), waardoor specifieke voorwaarden voor die doorgifte vereist zijn (zie artikel 39 RGR).

In dit scenario is geen sprake van specifieke regels die deze verwerking door de rechtshandhavingsinstantie toestaan.

6.3. Noodzakelijkheid en evenredigheid

Het gebruik van de dienst door de rechtshandhavingsinstantie houdt in dat persoonsgegevens worden gedeeld met een particuliere entiteit die gebruik maakt van een database waarin op onbeperkte, grootschalige wijze persoonsgegevens worden verzameld. Er is geen verband tussen de verzamelde persoonsgegevens en de nagestreefde doelstelling van de rechtshandhavingsautoriteit. Het delen van gegevens door de rechtshandhavingsautoriteit met de particuliere entiteit betekent ook dat de autoriteit geen controle heeft over de door de particuliere entiteit verwerkte gegevens en dat het voor de betrokkenen heel moeilijk is om hun rechten uit te oefenen, aangezien zij niet weten dat hun gegevens op deze manier worden verwerkt. Dit legt de lat erg hoog voor situaties waarin een dergelijke verwerking zelfs maar zou kunnen plaatsvinden. Het is twijfelachtig of een doelstelling zou voldoen aan de eisen van de richtlijn, aangezien eventuele afwijkingen en beperkingen van het recht op privacy en gegevensbescherming alleen van toepassing zijn wanneer dat strikt noodzakelijk is. Het algemeen belang van doeltreffendheid bij de bestrijding van ernstige strafbare feiten kan op zichzelf de verwerking niet rechtvaardigen wanneer zulke grote hoeveelheden gegevens zonder onderscheid worden verzameld. Deze verwerking zou daarom niet voldoen aan de vereisten van noodzakelijkheid en evenredigheid.

6.4. Conclusie

Het ontbreken van duidelijke, nauwkeurige en voorzienbare regels die voldoen aan de vereisten van de artikelen 4 en 10 van de richtlijn, en het ontbreken van bewijs dat deze verwerking strikt noodzakelijk is om de beoogde doelstellingen te bereiken, leidt tot de conclusie dat het gebruik van deze applicatie niet zou voldoen aan de vereisten van noodzakelijkheid en evenredigheid en een onevenredige inmenging zou betekenen in het recht van betrokkenen op eerbiediging van het privéleven en de bescherming van persoonsgegevens uit hoofde van het Handvest.