Leitlinien 05/2022 über den Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung

Version 2.0

Angenommen am 26. April 2023

Versionsverlauf

Version 1.0	12. Mai 2022	Annahme der Leitlinien zur öffentlichen Konsultation
Version 2.0	26. April 2023	Annahme der Leitlinien nach öffentlicher Konsultation

Inhaltsverzeichnis

ZUSAMMENFASSUNG

Immer mehr Strafverfolgungsbehörden verwenden bereits Gesichtserkennungstechnologie oder beabsichtigen deren Verwendung. Diese Technologie, mit der Personen **authentifiziert** oder **identifiziert** werden können, lässt sich auf Videos (z. B. Videoüberwachungsanlagen) oder Fotos anwenden. Sie kann für verschiedenen Zwecke eingesetzt werden, um unter anderem nach Personen auf polizeilichen Fahndungslisten zu suchen oder um die Bewegungen von Menschen im öffentlichen Raum zu überwachen.

Gesichtserkennungstechnologie beruht auf der Verarbeitung **biometrischer Daten**, umfasst also die Verarbeitung besonderer Kategorien personenbezogener Daten. Gesichtserkennungstechnologie verwendet oftmals Komponenten **künstlicher Intelligenz** (KI) oder maschinellen Lernens (ML). Dies ermöglicht die Verarbeitung großer Datenmengen, birgt jedoch auch die Gefahr von Diskriminierung und falschen Ergebnissen. Gesichtserkennungstechnologie kann in kontrollierten One-to-One-Situationen, aber auch in großen Menschenmengen und an wichtigen Verkehrsknotenpunkten eingesetzt werden.

Für die Strafverfolgungsbehörden ist die Gesichtserkennungstechnologie eine **sensible Technologie**. Strafverfolgungsbehörden sind mit Hoheitsgewalt ausgestattete ausführende Behörden. Gesichtserkennungstechnologie greift in der Regel – auch über das Recht auf Schutz personenbezogener Daten hinaus – in Grundrechte ein, was unseren gesellschaftlichen und demokratischen politischen Zusammenhalt gefährden kann.

Für den Datenschutz im Bereich der Strafverfolgung gelten die **Anforderungen der JI-Datenschutzrichtlinie**. Die JI-Datenschutzrichtlinie gibt einen gewissen Rahmen für den Einsatz von Gesichtserkennungstechnologie vor, insbesondere in Artikel 3 Absatz 13 (Begriff „biometrische Daten“), Artikel 4 (Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten), Artikel 8 (Rechtmäßigkeit der Verarbeitung), Artikel 10 (Verarbeitung besonderer Kategorien personenbezogener Daten) und Artikel 11 (Automatisierte Entscheidungsfindung im Einzelfall) der JI-Datenschutzrichtlinie.

Bei der Anwendung von Gesichtserkennungstechnologie können auch mehrere andere Grundrechte berührt sein. Deshalb ist die **Charta der Grundrechte der Europäischen Union** („Charta“) für die Auslegung der JI-Datenschutzrichtlinie von wesentlicher Bedeutung, insbesondere das Recht auf Schutz personenbezogener Daten in Artikel 8 der Charta, aber auch die Achtung des Privat- und Familienlebens in Artikel 7 der Charta.

Gesetzgeberische Maßnahmen, die als Rechtsgrundlage für die Verarbeitung personenbezogener Daten dienen, greifen unmittelbar in die in den Artikeln 7 und 8 der Charta garantierten Rechte ein. Die Verarbeitung biometrischer Daten stellt für sich genommen unter allen Umständen stets einen schweren Eingriff dar. Dies gilt unabhängig vom jeweiligen Verarbeitungsergebnis (z. B. einem positiven Abgleich („Treffer“)). Jede Einschränkung der Ausübung der Grundrechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten.

Die Rechtsgrundlage muss **hinreichend klar formuliert** sein, damit sie den Bürgern angemessenen Aufschluss darüber gibt, unter welchen Voraussetzungen und Umständen die Behörden zu derartigen Datenerhebungs- und geheimen Überwachungsmaßnahmen befugt sind. Würde lediglich die Generalklausel in Artikel 10 der JI-Datenschutzrichtlinie in innerstaatliches Recht umgesetzt, so würde es an Bestimmtheit und Vorhersehbarkeit mangeln.

Vor Erlass einer neuen Rechtsgrundlage für jegliche Form der Verarbeitung biometrischer Daten, bei der Gesichtserkennung verwendet wird, sollte der nationale Gesetzgeber die zuständige Aufsichtsbehörde für den Datenschutz **konsultieren**.

Gesetzgeberische Maßnahmen müssen **geeignet** sein, die mit dem in Rede stehenden Gesetz verfolgten legitimen Zielsetzungen zu erreichen. Eine **dem Gemeinwohl dienende Zielsetzung** – wie grundlegend diese auch sein mag – kann, für sich genommen, keine Grundrechtseinschränkungen rechtfertigen. Gesetzgeberische Maßnahmen sollten **differenzieren** und die Zielgruppe im Lichte der Zielsetzung (z. B. der Bekämpfung bestimmter schwerer Straftaten) bestimmen. Gilt die Vorschrift allgemein – ohne jede Differenzierung, Beschränkung oder Ausnahme – für alle Personen, so verstärkt das den Grundrechtseingriff. Der Eingriff wird auch verstärkt, wenn die Datenverarbeitung einen erheblichen Teil der Bevölkerung betrifft.

Die Daten müssen auf solche Weise verarbeitet werden, dass Anwendbarkeit und Wirksamkeit der unionsrechtlichen Datenschutzvorschriften und -grundsätze gewährleistet sind. In der Einzelfallbetrachtung sind in der **Bewertung der Erforderlichkeit und Verhältnismäßigkeit** auch alle in Betracht kommenden Auswirkungen auf andere Grundrechte zu ermitteln und zu berücksichtigen. Werden Daten systematisch verarbeitet, ohne dass dies den betroffenen Personen bekannt ist, so entsteht voraussichtlich ein **allgemeines Gefühl der ständigen Überwachung**. Das kann davor abschrecken, einige oder sämtliche Grundrechte auszuüben, etwa die Rechte aus Artikel 1 (Würde des Menschen), Artikel 10 (Gedanken-, Gewissens- und Religionsfreiheit), Artikel 11 (Freiheit der Meinungsäußerung) und Artikel 12 (Versammlungs- und Vereinigungsfreiheit) der Charta.

Die Verarbeitung besonderer Kategorien von Daten wie zum Beispiel biometrischer Daten kann nur als „**unbedingt erforderlich**“ (Artikel 10 JI-Datenschutzrichtlinie) angesehen werden, wenn der Eingriff in den Schutz personenbezogener Daten und die damit verbundene Grundrechtseinschränkung auf das unbedingt erforderliche (d. h. unverzichtbare) Maß beschränkt ist, was jede Verarbeitung allgemeiner oder systematischer Art ausschließt.

Aus dem Umstand, dass die betroffene Person ein Foto **offensichtlich öffentlich gemacht** hat (Artikel 10 JI-Datenschutzrichtlinie), folgt nicht, dass die damit verbundenen biometrischen Daten, die sich durch besondere technische Mittel dem Foto entnehmen lassen, als offensichtlich öffentlich gemacht anzusehen sind. Standardeinstellungen eines Dienstes (z. B. die öffentliche Zurverfügungstellung von Templates) oder das Fehlen einer Wahlmöglichkeit (z. B. die öffentliche Zurverfügungstellung von Templates, ohne dass der Nutzer diese Einstellung ändern kann) sollten in keiner Weise so ausgelegt werden, dass damit Daten offensichtlich öffentlich gemacht wurden.

In Artikel 11 der JI-Datenschutzrichtlinie ist die **automatisierte Entscheidungsfindung im Einzelfall** geregelt. Beim Einsatz von Gesichtserkennungstechnologie werden besondere Datenkategorien verwendet, was, je nachdem, auf welche Weise und zu welchem Zweck die Gesichtserkennungstechnologie angewendet wird, zu Profiling führen kann. Profiling, das zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist nach dem Unionsrecht und Artikel 11 Absatz 3 der JI-Datenschutzrichtlinie auf jeden Fall zu verbieten.

Artikel 6 der JI-Datenschutzrichtlinie betrifft die Notwendigkeit der **Unterscheidung verschiedener Kategorien betroffener Personen**. Im Falle betroffener Personen, bei denen es keine Anzeichen dafür gibt, dass ihr Verhalten eine Verbindung – und sei es auch nur eine mittelbare oder entfernte Verbindung – zum legitimen Ziel der JI-Datenschutzrichtlinie aufweisen könnte, lässt sich ein Eingriff höchstwahrscheinlich nicht rechtfertigen.

Nach dem **Grundsatz der Datenminimierung** (Artikel 4 Absatz 1 Buchstabe e der JI-Datenschutzrichtlinie) ist es zudem erforderlich, Videomaterial, das für den Zweck der Verarbeitung nicht relevant ist, stets vor dem Einsatz zu löschen oder zu anonymisieren (z. B. durch Unkenntlichmachung ohne nachträgliche Möglichkeit der Datenwiederherstellung).

Bevor der Verantwortliche mit der Datenverarbeitung mittels Gesichtserkennungstechnologie beginnt, muss er stets genau bedenken, auf welche Weise er die Anforderungen hinsichtlich der **Rechte der betroffenen Person** erfüllt (bzw., ob er diese überhaupt erfüllen kann); schließlich geht es bei Gesichtserkennungstechnologie oftmals darum, besondere Kategorien personenbezogener Daten zu verarbeiten, ohne dass es zu einer direkten Interaktion mit der betroffenen Person kommt.

Betroffene können ihre Rechte nur wirksam ausüben, wenn der Verantwortliche seine **Informationspflichten** erfüllt (Artikel 13 der JI-Datenschutzrichtlinie). Bei der Beurteilung, ob es sich um einen „besonderen Fall" im Sinne von Artikel 13 Absatz 2 der JI-Datenschutzrichtlinie handelt, sind mehrere Faktoren zu berücksichtigen, unter anderem, ob personenbezogene Daten ohne Wissen der betroffenen Person erhoben werden; schließlich ist den betroffenen Personen die wirksame Ausübung ihrer Rechte nur möglich, wenn sie von der Datenerhebung wissen. Sollte die Entscheidungsfindung allein auf Gesichtserkennungstechnologie beruhen, müssen die betroffenen Personen über die Funktionsweise der automatisierten Entscheidungsfindung informiert werden.

Bei **Auskunftsverlangen**, die gespeicherte biometrische Daten betreffen, die unter Einhaltung des Grundsatzes der Datenminimierung auch mittels alphanumerischer Daten mit einer Identität verknüpft sind, sollte es der zuständigen Behörde möglich sein, solche Auskunftsverlangen durch Suche nach den betreffenden alphanumerischen Daten zu beantworten, ohne eine weitere Verarbeitung biometrischer Daten anderer Personen zu starten (d. h. durch eine auf Gesichtserkennungstechnologie gestützte Datenbanksuche).

Besonders gravierende Risiken für betroffene Personen ergeben sich, wenn unrichtige Daten in einer polizeilichen Datenbank gespeichert und/oder mit anderen Stellen ausgetauscht werden. Der Verantwortliche muss gespeicherte Daten und Gesichtserkennungstechnologie erforderlichenfalls **berichtigen** (vgl. auch Erwägungsgrund 47 der JI-Datenschutzrichtlinie).

Besondere Bedeutung kommt dem Recht auf **Einschränkung** zu, wenn Gesichtserkennungstechnologie (die auf einem oder mehreren Algorithmen beruht und deshalb niemals ein definitives Ergebnis liefert) in Situationen eingesetzt wird, in denen große Datenmengen erhoben werden, bei denen die Richtigkeit und Qualität der Identifizierung schwanken kann.

Artikel 27 der JI-Datenschutzrichtlinie schreibt zwingend vor, dass vor dem Einsatz von Gesichtserkennungstechnologie eine **Datenschutz-Folgenabschätzung (DSFA)** durchzuführen ist. Der EDSA empfiehlt als vertrauens- und transparenzsteigernde Maßnahme, die Ergebnisse solcher DSFA oder zumindest deren wichtigste Erkenntnisse und Schlussfolgerungen zu veröffentlichen.

Die meisten Fälle, in denen Gesichtserkennungstechnologie eingesetzt oder verwendet wird, bergen hohe inhärente Risiken für die Rechte und Freiheiten der betroffenen Personen. Eine Behörde, die Gesichtserkennungstechnologie einsetzen will, sollte die zuständige Aufsichtsbehörde **konsultieren**, bevor das System eingesetzt wird.

Wegen der Einzigartigkeit biometrischer Daten sollten Behörden, die Gesichtserkennungstechnologie implementieren und/oder verwenden, besonders auf die in Artikel 29 der JI-Datenschutzrichtlinie vorgeschriebene **Sicherheit der Verarbeitung** achten. Strafverfolgungsbehörden sollten insbesondere sicherstellen, dass das System den einschlägigen Normen genügt und Maßnahmen zum Schutz

biometrischer Templates implementiert sind. Die Datenschutzgrundsätze und Garantien müssen in die Technologie eingebettet sein, bevor mit der Verarbeitung personenbezogener Daten begonnen wird. Das bedeutet, dass eine Strafverfolgungsbehörde, auch wenn sie Gesichtserkennungstechnologie externer Anbieter anwenden und benutzen will, sicherstellen muss (z. B. im Vergabeverfahren), dass ausschließlich Gesichtserkennungstechnologie, die auf den Grundsätzen des **Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen** aufbaut, zum Einsatz kommt.

Protokollierung (vgl. Artikel 25 der JI-Datenschutzrichtlinie) ist eine wichtige Garantie für die Überprüfung der Rechtmäßigkeit der Verarbeitung, sei es intern (d. h. durch Eigenüberwachung des betreffenden Verantwortlichen/Auftragsverarbeiters) oder durch externe Aufsichtsbehörden. Im Zusammenhang mit Gesichtserkennungssystemen wird empfohlen, auch bei Änderungen der Referenzdatenbank sowie bei Identifikations- oder Verifizierungsversuchen den Nutzer, das Ergebnis und den Konfidenz-Score zu protokollieren. Die Protokollierung ist jedoch nur eines von mehreren wesentlichen Elementen des **Grundsatzes der Rechenschaftspflicht** (vgl. Artikel 4 Absatz 4 der JI-Datenschutzrichtlinie). Der Verantwortliche muss nachweisen können, dass die Verarbeitung den in Artikel 4 Absätze 1 bis 3 der JI-Datenschutzrichtlinie verankerten grundlegenden Datenschutzgrundsätzen genügt.

Der EDSA erinnert daran, dass er gemeinsam mit dem EDSB gefordert hat, bestimmte Arten der Verarbeitung zu **verbieten**, nämlich die Verarbeitung in Zusammenhang mit (1) biometrischer Fernidentifizierung natürlicher Personen im frei zugänglichen öffentlichen Raum, (2) KI-unterstützten Gesichtserkennungssystemen, die natürliche Personen nach biometrischen Merkmalen in Cluster eingruppieren, etwa nach ethnischer Zugehörigkeit, Geschlecht ebenso wie nach politischer oder sexueller Orientierung oder sonstigen Merkmalen, die zu den verbotenen Diskriminierungsgründen zählen, (3) der Verwendung von Gesichtserkennung oder vergleichbaren Technologien zur Erkennung der Emotionen natürlicher Personen sowie (4) der Verarbeitung personenbezogener Daten zu Strafverfolgungszwecken, welche auf einer Datenbank massenhaft und unterschiedslos – z. B. durch Auslesen („Scrapen“) online zugänglicher Fotos und Gesichtsbildnisse – erfasster personenbezogener Daten beruhen würde.

Eine zentrale Garantie für die in Rede stehenden Grundrechte ist die **wirksame Aufsicht** durch die zuständigen Aufsichtsbehörden für den Datenschutz. Die Mitgliedstaaten müssen deshalb sicherstellen, dass die Aufsichtsbehörden mit geeigneten und ausreichenden Mitteln für die Wahrnehmung ihrer Aufgaben ausgestattet sind.

Adressat dieser Leitlinien sind die Gesetzgeber auf Unions- und nationaler Ebene sowie die Strafverfolgungsbehörden und ihre Beamten, die Gesichtserkennungssysteme implementieren und verwenden. Die Leitlinien richten sich an natürliche Personen, soweit diese ein allgemeines Interesse haben oder betroffene Personen sind, insbesondere was ihre Rechte als betroffene Personen angeht.

Mit diesen **Leitlinien soll** über bestimmte Eigenschaften der Gesichtserkennungstechnologie sowie den einschlägigen rechtlichen Rahmen im Zusammenhang mit der Strafverfolgung (insbesondere über die JI-Datenschutzrichtlinie) informiert werden.

- Darüber hinaus enthalten sie ein **Tool zur ersten Einstufung der Sensibilität eines gegebenen Anwendungsfalls** (Anhang I).
- Außerdem gibt es einen **Praxisleitfaden für Strafverfolgungsbehörden, die ein Gesichtserkennungssystem beschaffen und betreiben wollen** (Anhang II).

- Die Leitlinien umfassen auch mehrere typische **Anwendungsfälle und eine Auflistung zahlreicher relevanter Erwägungen**, insbesondere für die Prüfung der Erforderlichkeit und Verhältnismäßigkeit (Anhang III).

1 EINLEITUNG

1. Gesichtserkennungstechnologie ermöglicht es, Menschen anhand ihres Gesichts automatisch zu erkennen. Oftmals beruht Gesichtserkennungstechnologie auf künstlicher Intelligenz wie zum Beispiel auf Technologien des maschinellen Lernens. Gesichtserkennungstechnologie wird zunehmend in verschiedenen Bereichen getestet und auch eingesetzt: von der Nutzung durch Einzelpersonen bis zur Verwendung in privaten Organisationen und in der öffentlichen Verwaltung. Auch Strafverfolgungsbehörden rechnen mit einem Nutzen aus dem Einsatz von Gesichtserkennungstechnologie. Die Technologie verspricht Lösungen für relativ neue Probleme, etwa Ermittlungen, bei denen große Mengen von Beweismaterial anfallen, aber auch für bekannte Probleme, insbesondere das Problem der unzureichenden Personalausstattung für Beobachtungs- und Durchsuchungsaufgaben.

2. Das gestiegene Interesse an Gesichtserkennungstechnologie gilt zum großen Teil ihrer Effizienz und Skalierbarkeit. Dies geht jedoch mit den – ebenfalls sehr großen – Nachteilen einher, die der Technologie und ihrer Anwendung innewohnen. So ist es zwar möglich, auf Knopfdruck Tausende personenbezogene Datensätze zu analysieren, doch schon geringfügige Effekte algorithmischer Diskriminierung oder Fehlidentifizierung können zu erheblichen Beeinträchtigungen des Verhaltens und Lebensalltags einer hohen Zahl von Personen führen. Die enorme Menge der Verarbeitung personenbezogener Daten (insbesondere biometrischer Daten) ist ein weiterer Hauptaspekt der Gesichtserkennungstechnologie, denn die Verarbeitung personenbezogener Daten stellt einen Eingriff in das Grundrecht auf Schutz personenbezogener Daten aus Artikel 8 der Charta der Grundrechte der Europäischen Union (Charta) dar.

3. Wenn Strafverfolgungsbehörden Gesichtserkennungstechnologie anwenden, wird dies erhebliche Auswirkungen auf Einzelpersonen und Personengruppen (u. a. Minderheiten) haben. Zum Teil ist dies bereits erkennbar. Die Auswirkungen werden auch unser Zusammenleben und unseren gesellschaftlichen und demokratischen politischen Zusammenhalt, in dem Pluralismus und politischer Opposition große Bedeutung zukommen, spürbar verändern. Dem Recht auf Schutz personenbezogener Daten als Voraussetzung für die Garantie anderer Grundrechte kommt hier eine Schlüsselrolle zu. Bei Anwendung von Gesichtserkennungstechnologie ist die Wahrscheinlichkeit eines Grundrechtseingriffs, der über das Recht auf den Schutz personenbezogener Daten hinausgeht, recht hoch.

4. Deshalb hält es der EDSA für wichtig, sich zur laufenden Einbeziehung von Gesichtserkennungstechnologie im Bereich der Strafverfolgung, die der Strafverfolgungsrichtlinie[1] bzw. den zu deren Umsetzung dienenden innerstaatlichen Rechtsvorschriften unterliegt, zu äußern und diese Leitlinien vorzulegen. Die Leitlinien sollen den Gesetzgebern auf Unions- und nationaler Ebene wie auch den Strafverfolgungsbehörden und ihren Beamten die für die Implementierung und Verwendung von Gesichtserkennungssystemen relevanten Informationen liefern. Der

[1] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

Anwendungsbereich dieser Leitlinien beschränkt sich auf Gesichtserkennungstechnologie. Wenn Strafverfolgungsbehörden auf biometrische Daten gestützte personenbezogene Daten in anderer Form verarbeiten, insbesondere durch Fernverarbeitung, können sich allerdings ähnliche oder zusätzliche Risiken für Einzelpersonen, Gruppen und Gesellschaft ergeben. Je nach den Umständen mögen einige Aspekte dieser Leitlinien auch für solche Fälle nützlich sein. Letztlich mögen hierin auch diejenigen, die sich allgemein oder als betroffene Personen für das Thema interessieren, wichtige Informationen finden, insbesondere über die Rechte betroffener Personen.

5. Die Leitlinien bestehen aus dem Hauptdokument sowie drei Anhängen. Im vorliegenden Hauptdokument werden die Technologie und der einschlägige rechtliche Rahmen vorgestellt. Anhang I enthält eine Vorlage, in der einige der zentralen Aspekte aufgeführt sind, nach denen die Schwere des Grundrechtseingriffs für einen bestimmten Anwendungsbereich eingestuft werden kann. Für Strafverfolgungsbehörden, die ein Gesichtserkennungssystem beschaffen oder betreiben möchten, gibt es in Anhang II einen Praxisleitfaden. Je nachdem, in welchem Bereich Gesichtserkennungstechnologie angewendet werden soll, sind verschiedene Gesichtspunkte zu berücksichtigen. Anhang III enthält mehrere hypothetische Szenarien und die jeweils relevanten Erwägungen.

2 TECHNOLOGIE

2.1 Eine biometrische Technologie, zwei verschiedene Funktionen

6. Gesichtserkennung ist eine probabilistische Technologie zur automatischen Erkennung natürlicher Personen anhand ihres Gesichts mit den Zielen der Authentifizierung oder Identifizierung.

7. Die Gesichtserkennungstechnologie fällt in die übergeordnete Kategorie biometrischer Technologien. Die Biometrie umfasst sämtliche automatisierten Prozesse, die zur Personenerkennung anhand quantifizierter physischer, physiologischer oder Verhaltenseigenschaften (Fingerabdrücke, Irisstruktur, Stimme, Gangbild, Blutgefäßmuster usw.) verwendet werden. Diese Eigenschaften werden als „biometrische Daten“ bezeichnet, weil sie die eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen.

8. Dies ist der Fall bei menschlichen Gesichtern oder, genauer gesagt, bei deren technischer Verarbeitung mittels Gesichtserkennungsgeräten: Aus der Abbildung eines Gesichts (etwa einem Foto oder Video) – man nennt dies ein biometrisches „Sample“ – lässt sich eine digitale Wiedergabe bestimmter Charakteristika dieses Gesichts extrahieren (dies nennt man ein „Template“).

9. Ein biometrisches Template ist eine digitale Darstellung der eindeutigen Merkmale, die aus einem biometrischen Sample extrahiert wurden und in einer biometrischen Datenbank gespeichert werden können[2]. Dieses Template, das eindeutig und für jeden Menschen spezifisch sein soll, ist im Prinzip von unbegrenzter zeitlicher Gültigkeit[3]. In der Erkennungsphase vergleicht das Gerät dieses Template mit anderen Templates, die entweder zuvor erstellt oder aber direkt aus biometrischen Samples (z. B. einem in einem Bild, Foto oder Video gefundenen Gesicht) errechnet werden. Die „Gesichtserkennung“ ist also ein Verfahren mit zwei Schritten: Im ersten Schritt wird das Gesichtsbild erfasst und in ein Template umgewandelt; im zweiten Schritt erfolgt die Erkennung dieses Gesichts, indem das Template mit einem oder mehreren anderen Templates verglichen wird.

[2] Guidelines on facial recognition, Consultative Committee of Convention 108 the Convention for the protection of individuals with regard to automatic processing of personal data, Europarat, Juni 2021.
[3] Dies kann von der Art der Biometrie und dem Alter der betroffenen Personen abhängig sein.

10. Wie jedes biometrische Verfahren kann die Gesichtserkennung zwei verschiedene Funktionen erfüllen:

    - die **Authentifikation** einer Person, die darauf abzielt, zu bestätigen, dass die Person diejenige ist, für die sie sich ausgibt. In diesem Fall wird das System ein zuvor hinterlegtes (z. B. auf einer Smartcard oder in einem biometrischen Reisepass gespeichertes) biometrisches Template oder Sample mit einem einzigen Gesicht vergleichen, zum Beispiel mit dem Gesicht eines an einer Kontrollstelle erschienenen Menschen; dabei geht es dabei, zu überprüfen, ob es sich bei der abgebildeten und bei der erschienenen Person um dieselbe Person handelt. Diese Funktion beruht also auf dem Abgleich von zwei Templates. Dies wird auch als One-to-One-**Verifizierung** bezeichnet.

    - die **Identifizierung** einer Person, die darauf abzielt, eine Person in einer Menschengruppe, in einem bestimmten Bereich, auf einem Bild oder in einer Datenbank zu finden. In diesem Fall muss das System jedes erfasste Gesicht verarbeiten, ein biometrisches Template erzeugen und dann prüfen, ob dieses eine Übereinstimmung („Treffer“) mit einer dem System bekannten Person ergibt. Diese Funktion beruht also auf dem Abgleich eines Templates mit einer Datenbank von Templates oder Samples (Vergleichsbasis). Dies wird auch als One-to-Many-Identifikation bezeichnet. So kann zum Beispiel ein aufgezeichneter Personenname (Nachname, Vorname) mit einem Gesicht in Verbindung gebracht werden, wenn der Abgleich mit einer Datenbank erfolgt, in der Fotos mit Nachnamen und Vornamen verknüpft sind. Es kann auch darum gehen, jemanden, der sich in einer Menge bewegt, zu verfolgen, ohne dass notwendigerweise eine Verbindung zur zivilrechtlichen Identität der Person hergestellt wird.

11. In beiden Fällen geht es bei den zur Gesichtserkennung verwendeten Techniken um eine Schätzung, wie sehr die Templates – das Template, das verglichen wird, und eines oder mehrere als Vergleichsbasis dienende Templates – übereinstimmen. Die Techniken sind probabilistisch: Aus dem Abgleich wird abgeleitet, dass es sich bei der Person mit höherer oder geringerer Wahrscheinlichkeit tatsächlich um die zu authentifizierende oder zu identifizierende Person handelt. Übersteigt diese Wahrscheinlichkeit einen gewissen vom Nutzer oder Entwickler des Systems festgelegten Schwellenwert im System, so nimmt das System an, dass es sich um eine Übereinstimmung (Treffer) handelt.

12. Auch wenn die beiden Funktionen – Authentifikation und Identifikation – verschieden sind, beziehen sie sich doch beide auf die Verarbeitung biometrischer Daten einer identifizierten oder identifizierbaren natürlichen Person; es handelt sich also um eine Verarbeitung personenbezogener Daten, genauer gesagt um eine Verarbeitung besonderer Kategorien personenbezogener Daten.

13. Die Gesichtserkennung ist Teil eines breiteren Spektrums von Techniken zur Videobildverarbeitung. Es gibt Videokameras, mit denen man Menschen in einem festgelegten Bereich, insbesondere deren Gesichter, filmen kann; damit ist es jedoch nicht möglich, Einzelpersonen automatisch zu erkennen. Dasselbe gilt für einfache Fotografie: Eine Kamera ist kein Gesichtserkennungssystem, weil Fotos, auf denen Menschen abgebildet sind, auf bestimmte Weise verarbeitet werden müssen, um daraus biometrische Daten zu extrahieren.

14. Auch sogenannte „smarte“ Kameras, die lediglich erkennen, dass es sich um ein Gesicht handelt, stellen nicht notwendigerweise ein Gesichtserkennungssystem dar. Digitale Techniken zur Erkennung von ungewöhnlichem Verhalten oder Gewalttätigkeit oder zur Emotionserkennung anhand von Gesichtsausdrücken oder sogar zur Erkennung von Silhouetten werfen durchaus wichtige Fragen hinsichtlich der Ethik und Wirksamkeit auf. Sofern sie aber nicht auf die eindeutige Personenidentifizierung abzielen und die damit verbundene Verarbeitung personenbezogener Daten keine besonderen Kategorien personenbezogener Daten betrifft, sind sie nicht als biometrische

Systeme zur Verarbeitung besonderer Kategorien personenbezogener Daten anzusehen. Diese Beispiele weisen jedoch einen gewissen Zusammenhang mit der Gesichtserkennung auf und unterliegen auf jeden Fall den Vorschriften für den Schutz personenbezogener Daten[4]. Erkennungssysteme dieser Art können auch in Verbindung mit anderen Systemen verwendet werden, die auf die Personenidentifikation abzielen, in welchem Falle sie als Gesichtserkennungstechnologie anzusehen sind.

15. Anders als zum Beispiel Systeme zur Videoerfassung und -verarbeitung, für die physische Geräte installiert werden müssen, ist die Gesichtserkennung mit einer Software möglich, die in bestehenden Systemen (Kameras, Bilddatenbanken usw.) implementiert werden kann. Eine solche Funktion lässt sich deshalb nicht nur an eine Vielzahl von Systemen anschließen oder über Schnittstellen verbinden, sondern auch mit anderen Funktionen kombinieren. Eine derartige Integration in bereits bestehende Infrastruktur erfordert besondere Vorsicht, weil die Gesichtserkennungstechnologie unauffällig benutzt und leicht versteckt werden könnte, was bestimmte Gefahren birgt[5].

2.2 Vielfältiges Spektrum von Zwecken und Anwendungen

16. Außerhalb des Anwendungsbereichs dieser Leitlinien und der JI-Datenschutzrichtlinie kann Gesichtserkennung für verschiedenste Zwecke verwendet werden, sowohl gewerblich als auch für die Zwecke der öffentlichen Sicherheit und Strafverfolgung. Sie lässt sich in vielen verschiedenen Zusammenhängen anwenden: im persönlichen Verhältnis zwischen Nutzer und Dienst (Zugang zu einer App), für den Zugang zu einem bestimmten Ort (physische Personenfilterung) oder ohne besondere Einschränkung im öffentlichen Raum (Gesichtserkennung in Echtzeit). Personen jeglicher Art können von der Anwendung betroffen sein: z. B. Kunden, die einen Dienst in Anspruch nehmen, Angestellte, einfache Zuschauer, zur Fahndung ausgeschriebene Personen oder jemand, der an einem Gerichts- oder Verwaltungsverfahren beteiligt ist. Einige Anwendungsarten sind bereits allgemein üblich und weit verbreitet; andere sind bislang noch in der Erprobung oder reine Gedankenspiele. In diesen Leitlinien wird nicht auf alle derartigen Verwendungen und Anwendungen eingegangen werden. Der EDSA erinnert jedoch daran, dass eine Implementierung stets nur dann in Betracht kommt, wenn sie dem einschlägigen Rechtsrahmen, insbesondere der DSGVO und den einschlägigen einzelstaatlichen Rechtsvorschriften, genügt.[6] Selbst im Rahmen der JI-Datenschutzrichtlinie können Daten, die mittels Gesichtserkennungstechnologie verarbeitet werden, über die Funktionen der Authentifikation oder Identifikation hinaus auch für andere Zwecke weiterverarbeitet werden, zum Beispiel für die Kategorisierung.

17. Man kann sich ein breites Spektrum potenzieller Verwendungen vorstellen, die den Menschen ein ganz unterschiedliches Maß an Kontrolle über ihre personenbezogenen Daten, an wirksamen Mitteln zur Ausübung dieser Kontrolle und an Rechten, diese Technologie aus eigener Initiative zu nutzen, bieten, die (im Falle der Erkennung oder Nichterkennung) unterschiedliche Folgen für die Menschen haben und die mit unterschiedlich umfangreicher Verarbeitung verbunden sind. Gesichtserkennung, die auf einem Template beruht, das auf einem der betreffenden Person gehörenden persönlichen Gerät (Smartcard, Smartphone usw.) gespeichert ist, und die zur Authentifikation und ausschließlich zum persönlichen Gebrauch über eine eigens dafür vorgesehene Schnittstelle verwendet wird, birgt nicht

[4] Artikel 10 der JI-Datenschutzrichtlinie (oder Artikel 9 DSGVO) findet jedoch Anwendung auf Systeme, die dazu verwendet werden, Personen anhand biometrischer Daten in Cluster einzugruppieren, etwa nach ethnischer Zugehörigkeit, politischer oder sexueller Orientierung oder sonstigen besonderen Kategorien personenbezogener Daten.

[5] Dies gilt zum Beispiel für am Körper getragene Kameras, die in der Praxis immer häufiger benutzt werden.

[6] Vgl. dazu auch Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, angenommen am 29. Januar 2020.

dieselben Risiken wie beispielsweise eine Verwendung zu Identifikationszwecken in nicht kontrollierter Umgebung, ohne aktive Mitwirkung der betroffenen Personen, bei der das Template jedes in den Überwachungsbereich gelangenden Gerichts mit den in einer Datenbank gespeicherten Templates aus einem breiten Querschnitt der Bevölkerung abgeglichen wird. Zwischen diesen beiden Extremen liegt ein sehr vielfältiges Spektrum von Verwendungen und damit verbundenen Problemen im Hinblick auf den Schutz der personenbezogenen Daten.

18. Zur weiteren Veranschaulichung des Zusammenhangs, in dem Gesichtserkennungstechnologien derzeit diskutiert oder für Authentifikations- oder Identifikationszwecke implementiert werden, hält es der EDSA für sinnvoll, einige Beispiele aufzuführen. Diese Beispiele dienen lediglich der Illustration und sie sind in keiner Weise als vorläufige Bewertung ihrer Konformität mit dem Besitzstand der Union auf dem Gebiet des Datenschutzes zu verstehen.

Beispiele für die Authentifikation mittels Gesichtserkennung

19. Die Authentifikation kann so gestaltet werden, dass die Nutzer die volle Kontrolle darüber haben – zum Beispiel zur Ermöglichung des Zugangs zu Diensten oder für ausschließlich auf private Wohnräume beschränkte Anwendungen. Sehr viele Smartphone-Benutzer machen davon Gebrauch, um ihr Gerät ohne Kennwort-Authentifizierung entsperren zu können.

20. Authentifikation per Gesichtserkennung kann auch dazu verwendet werden, die Identität einer Person, die öffentliche Leistungen oder Leistungen privater Anbieter in Anspruch nehmen möchte, zu prüfen. Derartige Verfahren bieten also die Möglichkeit, mit einer mobilen App (per Smartphone, Tablet usw.) eine digitale Identität zu schaffen, mit der dann online auf Verwaltungsleistungen zugegriffen werden kann.

21. Die Authentifikation per Gesichtserkennung kann auch darauf abzielen, den physischen Zugang zu einer oder mehreren vorab festgelegten Örtlichkeiten zu kontrollieren, zum Beispiel Gebäudeeingänge oder bestimmte Grenzübergangsstellen. Diese Funktion ist zum Beispiel in bestimmten Verarbeitungsvorgängen für die Zwecke des Grenzübergangs implementiert, bei denen das Gerät an der Grenzübergangsstelle das Gesicht der Person mit dem Bild in ihrem Identitätsdokument (Reisepass oder Aufenthaltserlaubnis) abgleicht.

Beispiele für die Identifikation mittels Gesichtserkennung

22. Die Identifikation ist auf vielerlei, noch vielfältigere Arten möglich. Dazu zählen insbesondere, wobei dies keine abschließende Aufzählung ist, die nachstehend aufgeführten Anwendungen, die zurzeit bereits in der EU zu sehen sind, ausprobiert oder geplant werden:

    - Suche nach der Identität einer nicht identifizierten Person (Opfer, Verdächtiger usw.) in einer Fotodatenbank;

    - Überwachung der Bewegung einer Person im öffentlichen Raum: Das Gesicht der Person wird mit den biometrischen Templates von Personen, die im überwachten Bereich reisen oder gereist sind, abgeglichen (zum Beispiel, wenn ein Gepäckstück vergessen oder eine Straftat begangen wurde);

    - Rekonstruktion der Reise einer Person und ihrer anschließenden Interaktionen mit anderen Personen (zum Beispiel durch zeitverzögerten Abgleich derselben Elemente, um die Kontaktpersonen zu identifizieren);

    - biometrische Fernidentifizierung zur Fahndung ausgeschriebener Personen im öffentlichen Raum: Alle von Videoschutzkameras live erfassten Gesichter werden in Echtzeit mit einer von den Sicherheitskräften geführten Datenbank abgeglichen;

- automatische Erkennung von Personen auf einem Bild, um zum Beispiel deren Beziehungen in einem sozialen Netzwerk, das diese Technik verwendet, zu erkennen. Das Bild wird mit den Templates aller Personen im Netzwerk, die ihre Einwilligung für diese Funktion erteilt haben, abgeglichen, um diese Beziehungen namentlich zu identifizieren;

- Zugang zu Diensten wie zum Beispiel Geldautomaten, die zur Kundenidentifikation das von einer Kamera erfasste Gericht mit der von der Bank geführten Gesichtsbilddatenbank abgleichen;

- Verfolgung der Reise eines Passagiers auf einer bestimmten Reiseetappe. Das in Echtzeit errechnete Template einer Person, die auf bestimmten Reiseetappen an Gates eincheckt (Gepäckabgabepunkte, Flugsteige usw.), wird mit den Templates bereits im System registrierter Personen abgeglichen.

23. Da die beobachteten Anwendungen weit über den Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung hinausgehen, ist eine umfassende Debatte und Strategie sicherlich geboten, um die Einheitlichkeit und Einhaltung des Besitzstands der EU auf dem Gebiet des Datenschutzes zu gewährleisten.

2.3 Zuverlässigkeit, Richtigkeit und Risiken für betroffene Personen

24. Wie bei jeder Technologie kann es auch bei der Gesichtserkennung Probleme geben, wenn es um die Implementierung geht, insbesondere was ihre Zuverlässigkeit und Effizienz für die Authentifikation und Identifikation angeht, aber auch insgesamt im Hinblick auf die Qualität und Richtigkeit der „Quelldaten“ und des Ergebnisses der mittels Gesichtserkennungstechnologie erfolgten Verarbeitung.

25. Für die betroffenen Personen bergen solche technologischen Probleme besondere Risiken, die im Bereich der Strafverfolgung umso wichtiger oder gravierender sind, wenn man die möglichen rechtlichen oder sonstigen vergleichbar schweren Folgen für die betroffenen Personen bedenkt. In diesem Zusammenhang scheint es angebracht, hervorzuheben, dass der Ex-post-Einsatz von Gesichtserkennungstechnologie nicht unbedingt sicherer ist, da Personen über längere Zeit und verschiedene Orte hinweg verfolgt werden können. Der Ex-post-Einsatz birgt deshalb besondere Risiken, die jeweils im Einzelfall zu prüfen sind[7].

26. So hat die Agentur der Europäischen Union für Grundrechte in ihrem Bericht 2019 darauf hingewiesen, dass „[d]en erforderlichen Grad an Genauigkeit für eine Software zur Gesichtserkennung festzulegen … eine Herausforderung [darstellt], da es viele unterschiedliche Formen für die Bewertung der Genauigkeit gibt und diese zudem von der Aufgabe, dem Zweck und dem Kontext des Einsatzes abhängt. Wird die Technologie an Orten eingesetzt, die von Millionen von Menschen besucht werden – wie Bahnhöfe oder Flughäfen –, kann schon eine relativ geringe Fehlerquote (z. B. 0,01 %)[8] bedeuten, dass Hunderte von Personen fälschlicherweise markiert werden. Wie in Abschnitt 3 beschrieben, besteht zudem bei bestimmten Kategorien von Personen möglicherweise eine höhere Wahrscheinlichkeit einer fehlerhaften Übereinstimmung als bei anderen. Es gibt unterschiedliche Möglichkeiten, die Fehlerquoten zu berechnen und zu interpretieren, weshalb Vorsicht geboten ist. Im Hinblick auf Genauigkeit und Fehler sind insbesondere für die Zwecke der Strafverfolgung die Fragen nach der Täuschungsanfälligkeit des Systems, beispielsweise durch gefälschte Gesichtsbilder (sogenanntes „Spoofing“), von Bedeutung.“[9]

[7] Vgl. dazu die Beispiele in Anhang III.

[8] Diese Trefferquote, die dem Bericht entnommen wurde, ist viel besser als die derzeitige Leistungsfähigkeit von Algorithmen in Anwendungen von Gesichtserkennungstechnologie.

[9] Gesichtserkennungstechnologien: grundrechtsrelevante Erwägungen im Rahmen der Strafverfolgung, Agentur der Europäischen Union für Grundrechte, 21. November 2019.

27. In diesem Kontext hält es der EDSA für wichtig, daran zu erinnern, dass Gesichtserkennungstechnologie, unabhängig davon, ob sie für Authentifikations- oder Identifikationszwecke eingesetzt wird, kein definitives Ergebnis liefert, sondern eine Aussage über die Wahrscheinlichkeit trifft, dass zwei Gesichter bzw. Bilder von Gesichtern zur selben Person gehören.[10] Dieses Ergebnis wird noch schlechter, wenn das für die Gesichtserkennung verwendete biometrische Sample von schlechter Qualität ist. Unscharfe Eingabebilder, Kameras mit niedriger Auflösung, Bewegung und schwaches Licht – all diese Faktoren können die Bildqualität beeinträchtigen. Andere Aspekte, die sich erheblich auf die Ergebnisse auswirken, sind Prävalenz und Spoofing, z. B., wenn Straftäter versuchen, Kameras auszuweichen oder die Gesichtserkennungstechnologie auszutricksen. Zahlreiche Studien haben auch gezeigt, dass derartige statistische Ergebnisse aus der algorithmischen Verarbeitung durch Bias verzerrt sein können, wobei sich solche Verzerrungen sowohl aus der Qualität der Quelldaten als auch aus den Trainingsdatenbanken oder anderen Faktoren, zum Beispiel der Wahl des Einsatzsorts, ergeben können. Hervorzuheben sind auch die Auswirkungen der Gesichtserkennungstechnologie auf andere Grundrechte, etwa auf die Achtung des Privat- und Familienlebens, auf die Freiheit der Meinungsäußerung und Informationsfreiheit sowie auf die Versammlungs- und Vereinigungsfreiheit usw.

28. Es ist daher unbedingt erforderlich, die Zuverlässigkeit und Richtigkeit der Gesichtserkennungstechnologie als Kriterium für die Beurteilung der Hauptdatenschutzgrundsätze gemäß Artikel 4 der JI-Datenschutzrichtlinie zu berücksichtigen, insbesondere was Fairness (Treu und Glauben) und Richtigkeit angeht.

29. Der EDSA betont, dass für hochwertige Algorithmen hochwertige Daten unerlässlich sind. Die Verantwortlichen müssen aber im Rahmen ihrer Rechenschaftspflicht auch gehalten sein, die algorithmische Verarbeitung regelmäßig und systematisch zu evaluieren, um insbesondere die Richtigkeit, Fairness und Zuverlässigkeit des Ergebnisses der Verarbeitung personenbezogener Daten sicherzustellen. Personenbezogene Daten, die dazu verwendet werden, Gesichtserkennungssysteme zu evaluieren, zu trainieren und weiterzuentwickeln, dürfen nur auf hinreichender Rechtsgrundlage und gemäß gemeinsamen Datenschutzgrundsätzen verarbeitet werden.

3 EINSCHLÄGIGER RECHTLICHER RAHMEN

30. Der Einsatz von Gesichtserkennungstechnologien geht notwendigerweise mit der Verarbeitung personenbezogener Daten einher; dabei werden auch besondere Datenkategorien verarbeitet. Dies hat unmittelbare oder mittelbare Auswirkungen auf mehrere der in der Charta der Grundrechte der Europäischen Union verankerten Grundrechte. Besonders betroffen ist der Bereich der Strafverfolgung und Strafjustiz. Deshalb sollten Gesichtserkennungstechnologien stets unter strikter Einhaltung der einschlägigen Rechtsvorschriften eingesetzt werden.

31. Im Folgenden wird aufgezeigt, was bei der Beurteilung künftiger Gesetzgebungs- und Verwaltungsmaßnahmen wie auch bei der Anwendung bestehender Rechtsvorschriften auf den Einsatz von Gesichtserkennungstechnologie im Einzelfall bedacht werden sollte. Die Relevanz der verschiedenen Anforderungen wird von den Umständen des Einzelfalls abhängen. Da es nicht möglich ist, alle künftigen Sachverhalte vorherzusehen, sind diese Informationen lediglich als Hilfestellung gedacht und nicht als erschöpfende Aufzählung aller relevanten Gesichtspunkte zu verstehen.

[10] Diese Wahrscheinlichkeit wird als „Konfidenz-Score“ bezeichnet.

3.1 Allgemeiner Rechtsrahmen – Die Charta der Grundrechte der Europäischen Union und die Europäische Menschenrechtskonvention (EMRK)

3.1.1 Anwendbarkeit der Charta

32. Die Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) richtet sich an die Organe, Einrichtungen und sonstigen Stellen der Union und an die Mitgliedstaaten, soweit diese das Recht der Union durchführen.

33. Die Regelung der Verarbeitung biometrischer Daten zu Strafverfolgungszwecken gemäß Artikel 1 Absatz 1 der JI-Datenschutzrichtlinie wirft unweigerlich die Frage nach der Einhaltung der Grundrechte auf, insbesondere im Hinblick auf die Achtung des Privatlebens und der Kommunikation (Artikel 7 der Charta) und das Recht auf Schutz personenbezogener Daten (Artikel 8 der Charta).

34. Bei der Erhebung und Analyse von Videoaufnahmen, auf denen natürliche Personen einschließlich ihrer Gesichter aufgezeichnet sind, werden zwangsläufig personenbezogene Daten verarbeitet. Die technische Bildverarbeitung erstreckt sich auch auf biometrische Daten. Werden Daten, die sich auf das Gesicht einer natürlichen Person beziehen, in Bezug auf Zeit und Raum verarbeitet, so kann die technische Verarbeitung Aufschluss über das Privatleben der betreffenden Personen geben. Daraus gezogene Schlussfolgerungen können die Rasse oder ethnische Herkunft einer Person, ihren Gesundheitszustand, ihre Religion, ihre Alltagsgewohnheiten, ihre dauerhaften oder vorübergehenden Wohnorte, ihre alltäglichen oder sonstigen Bewegungen, von ihr ausgeübte Tätigkeiten, ihre sozialen Beziehungen und die von ihr frequentierten sozialen Umfelder betreffen. Aus dem breiten Spektrum der Informationen, die durch Anwendung von Gesichtserkennungstechnologie gewonnen werden können, sind die möglichen Auswirkungen auf das Recht auf den Schutz personenbezogener Daten (Artikel 8 der Charta), aber auch auf das Recht auf Achtung des Privatlebens (Artikel 7 der Charta) klar zu ersehen.

35. Vor diesem Hintergrund ist die Vorstellung nicht abwegig, dass die Erhebung, Analyse und Weiterverarbeitung biometrischer Daten (Gesichtsdaten), um die es hier geht, Auswirkungen darauf haben könnte, wie Menschen ihre Handlungsfreiheit wahrnehmen – und zwar selbst dann, wenn sich ihre Handlungen in vollem Umfang im Rahmen des in einer freien und offenen Gesellschaft Zulässigen halten. Es sind auch gravierende Auswirkungen auf die Grundrechtsausübung denkbar, etwa auf die Ausübung der Rechte auf Gedanken-, Gewissens- und Religionsfreiheit, auf Freiheit der Meinungsäußerung und Informationsfreiheit sowie auf Versammlungs- und Vereinigungsfreiheit (Artikel 1, 10, 11 und 12 der Charta). Eine derartige Verarbeitung birgt aber auch andere Risiken, etwa das Risiko, dass die von den zuständigen Behörden erhobenen personenbezogenen Daten missbräuchlich genutzt werden, zum Beispiel durch rechtswidrigen Zugriff auf personenbezogene Daten, bei rechtswidriger Verwendung personenbezogener Daten oder bei Sicherheitsverletzungen usw. Die Risiken – etwa das Risiko eines rechtswidrigen Zugriffs und der rechtswidrigen Verwendung durch Polizeibeamte und andere Unbefugte – sind oftmals von der Verarbeitung und den Umständen, unter denen sie erfolgt, abhängig. Einige Risiken ergeben sich aber zwangsläufig aus der Einzigartigkeit biometrischer Daten. Adressen oder Telefonnummern kann die betroffene Person ändern, ihre einzigartigen Eigenschaften – ihr Gesicht oder ihre Iris – jedoch nicht. Würde unbefugt auf biometrische Daten zugegriffen oder würden diese versehentlich öffentlich, so wären die betreffenden Daten in ihrer Funktion als Passwörter oder kryptografische Schlüssel beeinträchtigt; sie könnten aber für weitere, nicht autorisierte Überwachungsmaßnahmen zum Schaden der betroffenen Person missbraucht werden.

3.1.2 Eingriff in die in der Charta verankerten Rechte

36. Die Verarbeitung biometrischer Daten stellt, für sich genommen, unter allen Umständen stets einen schweren Eingriff dar. Dies gilt unabhängig vom jeweiligen Verarbeitungsergebnis (z. B. einem positiven Abgleich („Treffer")). Die Verarbeitung ist selbst dann ein Eingriff, wenn im Falle eines Nicht-Treffers das biometrische Template nach dem Abgleich mit der Polizeidatenbank sofort gelöscht wird.

37. Der Eingriff in die Grundrechte betroffener Personen kann sich aus einem Rechtsakt ergeben, der die Beschränkung des betreffenden Grundrechts bezweckt oder bewirkt[11]. Er kann sich auch aus einer die Beschränkung des betreffenden Grundrechts bezweckenden oder bewirkenden Maßnahme einer öffentlichen Stelle oder gar einer zur Ausübung von Hoheitsgewalt ermächtigten privaten Rechtsperson ergeben.

38. Eine gesetzgeberische Maßnahme, die als Rechtsgrundlage für die Verarbeitung personenbezogener Daten dient, greift unmittelbar in die in den Artikeln 7 und 8 der Charta garantierten Rechte ein[12].

39. Die Verwendung von biometrischen Daten und insbesondere von Gesichtserkennungstechnologie berührt häufig auch die in Artikel 1 der Charta garantierte Menschenwürde. Die Menschenwürde verlangt, Menschen nicht zum bloßen Objekt zu machen. Mit Gesichtserkennungstechnologie werden Gesichtszüge – d. h. höchstpersönliche und die Existenz des betreffenden Menschen prägende Eigenschaften – durch Berechnungen in maschinenlesbare Form gebracht, um diese als menschliches Nummernschild oder als Identitätsausweis nutzen zu können; dadurch wird das Gesicht objektifiziert.

40. Soweit die jeweilige behördliche Videoüberwachung abschreckende Wirkung bezweckt oder bewirkt, kann eine solche Verarbeitung auch in andere Grundrechte eingreifen, etwa in die Rechte aus den Artikeln 10, 11 und 12 der Charta,

41. Hinzu kommen die potenziellen Risiken für die Rechte aus Artikel 47 und 48 der Charta (Recht auf ein unparteiisches Gericht und Unschuldsvermutung), die sich durch den Einsatz von Gesichtserkennungstechnologie durch Strafverfolgungsbehörden ergeben können und die ebenfalls sehr genau bedacht werden sollten. Das Ergebnis der Anwendung von Gesichtserkennungstechnologie (z. B. ein Treffer) führt möglicherweise nicht nur dazu, dass jemand weiteren Polizeimaßnahmen ausgesetzt ist, sondern könnte auch der maßgebliche Beweis in einem Gerichtsverfahren sein. Mängel der Gesichtserkennungstechnologie – zum Beispiel Bias, Diskriminierung oder Falschidentifikation („Falschtreffer") – können also gravierende Auswirkungen auf Strafverfahren haben. Es könnte dazu kommen, dass in der Beweiswürdigung dem Ergebnis der Anwendung der Gesichtserkennungstechnologie die meiste Bedeutung beigemessen wird, selbst wenn es gegenteilige Beweise gibt („Maschinengläubigkeit").

3.1.3 Rechtfertigung des Eingriffs

42. Artikel 52 Absatz 1 der Charta bestimmt, dass jede Einschränkung der Ausübung der in dieser Charta anerkannten Grundrechte und Freiheiten gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten muss. Nach dem Grundsatz der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

[11] EuGH, C-219/91 – Ter Voort, Slg. 1992 I-05485, Rn. 36 f.; EuGH, C-200/96 – Metronome, Slg. 1998 I-01953, Rn. 28.

[12] EuGH, C-594/12, Rn. 36; EuGH, C-291/12, Rn. 23 ff.

3.1.3.1 Gesetzlich vorgesehen

43. Gemäß Artikel 52 Absatz 1 der Charta bedarf es einer spezifischen Rechtsgrundlage. Diese Rechtsgrundlage muss hinreichend klar formuliert sein, damit die Bürger angemessenen Aufschluss darüber haben, unter welchen Voraussetzungen und Umständen die Behörden zu derartigen Maßnahmen der Datenerhebung und geheimen Überwachung befugt sind[13]. Sie muss mit angemessener Klarheit das Ausmaß und die Art und Weise der Ausübung des den öffentlichen Stellen eingeräumten Ermessens angeben, um das Mindestmaß an Schutz sicherzustellen, das Personen in einer demokratischen Gesellschaft nach dem Rechtsstaatsprinzip zusteht[14]. Überdies erfordert die Rechtmäßigkeit angemessene Garantien, um sicherzustellen, dass insbesondere die Rechte einer Person aus Artikel 8 der Charta geachtet werden. Diese Grundsätze gelten auch für die Verarbeitung personenbezogener Daten für die Zwecke der Evaluierung, des Trainings und der Weiterentwicklung von Gesichtserkennungssystemen.

44. Da biometrische Daten, die für die Zwecke der eindeutigen Identifikation einer natürlichen Person verarbeitet werden, eine besondere Datenkategorie im Sinne von Artikel 10 der JI-Datenschutzrichtlinie darstellen, bedürften die verschiedenen Anwendungen von Gesichtserkennungstechnologie in den meisten Fällen eines spezifischen Gesetzes, in dem die Anwendung und die Anwendungsvoraussetzungen genau vorgegeben sind. Dazu zählen insbesondere Angaben zur Art der Straftaten sowie ggf. zur erforderliche Schwere dieser Straftaten, um unter anderem geringfügige Vergehen wirksam auszuschließen.[15]

3.1.3.2 Wesensgehalt der in den Artikeln 7 und 8 der Charta verankerten Grundrechte auf Privatsphäre und Schutz personenbezogener Daten

45. Im Einzelfall muss die Grundrechtseinschränkung den Wesensgehalt des betreffenden Grundrechts achten. Der Wesensgehalt ist der unantastbare Kern des betreffenden Grundrechts[16]. Auch bei Einschränkungen eines Rechts darf die Menschenwürde nicht angetastet werden[17].

46. Anzeichen für eine mögliche Verletzung des unantastbaren Kerns sind:

- wenn eine Bestimmung Einschränkungen vorsieht, ohne das individuelle Verhalten einer Person oder Ausnahmefälle zu berücksichtigen[18];
- wenn der Rechtsweg ausgeschlossen ist oder behindert wird[19];
- wenn vor einer schweren Einschränkung die Umstände der betroffenen Person unberücksichtigt bleiben[20];
- hinsichtlich der Rechte aus den Artikeln 7 und 8 der Charta: wenn bei in großem Umfang erfolgender Erhebung von Kommunikations-Metadaten die darüber hinausgehende Kenntnisnahme vom Inhalt der elektronischen Kommunikation den Wesensgehalt dieser Rechte antasten könnte[21].
- hinsichtlich der Rechte aus den Artikeln 7, 8 und 11 der Charta: Vorschriften, mit denen den Anbietern eines öffentlichen Online-Zugangs zu Kommunikationsdiensten und den Betreibern von

[13] EGMR, Shimovolos v. Russia, § 68; Vukota-Bojić v. Switzerland.
[14] EGMR, Piechowicz v. Poland, § 212.
[15] Vgl. z. B. Urteile des EuGH in den Rechtssachen C-817/19 Ligue des droits humains, Rn. 151 f, C-207/16 Ministerio Fiscal, Rn. 56.
[16] EuGH C-279/09, Slg. 2010 I-13849, Rn. 60.
[17] Erläuterungen zur Charta der Grundrechte, Titel I, Erläuterung zu Artikel 1 – Würde des Menschen, ABl. C 303, 14.12.2007, S. 17-35.
[18] EuGH C-601/15, Rn. 52.
[19] EuGH C-400/10, Slg. 2010 I-08965, Rn. 55.
[20] EuGH C-408/03, Slg. 2006 I-02647, Rn. 68.
[21] EuGH C-203/15 – Tele2 Sverige, Rn. 101 unter Bezugnahme auf EuGH – C-293/12 und C-594/12, Rn. 39;

Hosting-Diensten eine allgemeine und unterschiedslose Vorratsspeicherung insbesondere von personenbezogenen Daten im Zusammenhang mit diesen Diensten auferlegt wird[22];

- hinsichtlich der Rechte aus Artikel 8 der Charta: wenn grundlegende Vorgaben des Datenschutzes und der Datensicherheit fehlen, könnte der Kern des Grundrechts angetastet sein[23].

3.1.3.3 Legitimes Ziel

47. Wie bereits in Abschnitt 3.1.3 erörtert, müssen Grundrechtseinschränkungen den von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

48. Von der Union anerkannt sind nicht nur die in Artikel 3 des Vertrags über die Europäische Union aufgeführten Ziele, sondern auch andere Interessen, die durch besondere Bestimmungen der Verträge[24] (d. h. u. a. im Raum der Freiheit, der Sicherheit und des Rechts, bei der Kriminalitätsprävention und -bekämpfung) geschützt werden. In ihren Beziehungen zum Rest der Welt sollte die Union zu Frieden und Sicherheit sowie zum Schutz der Menschenrechte beitragen.

49. Die Erfordernisse des Schutzes der Rechte und Freiheiten anderer beziehen sich auf die Rechte der Personen, die durch das Recht der Europäischen Union oder ihrer Mitgliedstaaten geschützt sind. Die Prüfung muss darauf abzielen, die Erfordernisse des Schutzes der verschiedenen Rechte in Einklang zu bringen und ein ausgewogenes Gleichgewicht zwischen ihnen zu erreichen[25].

3.1.3.4 Prüfung der Erforderlichkeit und Verhältnismäßigkeit

50. Geht es um Grundrechtseingriffe, so kann der Gestaltungsspielraum des nationalen wie auch des Unionsgesetzgebers eingeschränkt sein. Dabei ist eine Reihe von Faktoren zu beachten, z. B. der betroffene Bereich, das Wesen des jeweiligen durch die Charta gewährleisteten Rechts, die Art und Schwere des Eingriffs sowie dessen Zweck[26]. Gesetzgeberische Maßnahmen müssen geeignet sein, die mit dem in Rede stehenden Gesetz verfolgten legitimen Ziele zu erreichen. Die Maßnahme darf auch nicht die Grenzen dessen überschreiten, was zur Erreichung dieser Ziele geeignet und erforderlich ist[27]. Eine dem Gemeinwohl dienende Zielsetzung kann jedoch, so grundlegend sie auch sein mag, für sich genommen die Einschränkung eines Grundrechts nicht rechtfertigen[28].

51. Nach der ständigen Rechtsprechung des EuGH müssen sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken[29]. Dies ist nur der Fall, wenn sich der Zweck nicht mit weniger stark eingreifenden Mittel erreichen lässt. Alternativen, die je nach Zweck in Betracht kämen, wären etwa zusätzliches Personal, häufigere Streifengänge oder zusätzliche Straßenbeleuchtung; solche Alternativen sind genau anzugeben und zu prüfen. Gesetzgeberische Maßnahmen sollten differenzieren und ihr persönlicher

[22] EuGH C--511/18, La Quadrature du Net, Rn. 209 ff.
[23] EuGH – C-594/12, Rn. 40.
[24] Erläuterungen zur Charta der Grundrechte, Titel I, Erläuterung zu Artikel 52 – Würde des Menschen, ABl. C 303, 14.12.2007, S. 17-35.
[25] Jarass GrCh, 3. Aufl. 2016, EU-Grundrechte-Charta Artikel 52 Rn. 31-32.
[26] EuGH – C-594/12, Rn. 47 mit weiteren Nachweisen: vgl. entsprechend zu Artikel 8 EMRK, EGMR, S. and Marper v. the United Kingdom [GC], Nrn. 30562/04 und 30566/04, § 102, EMRK 2008-V.
[27] EuGH – C-594/12, Rn. 46 mit folgenden Nachweisen: Rechtssache C-343/09 Afton Chemical EU:C:2010:419, Rn. 45; Volker und Markus Schecke und Eifert, EU:C:2010:662, Rn. 74; Rechtssachen C-581/10 und C-629/10 Nelson und andere, EU:C:2012:657, Rn. 71; Rechtssache C-283/11 Sky Österreich, EU:C:2013:28, Rn. 50; sowie Rechtssache C-101/12 Schaible, EU:C:2013:661, Rn. 29.
[28] EuGH – C-594/12, Rn. 51.
[29] EuGH – C-594/12, Rn. 52 mit weiteren Nachweisen: Rechtssache C-473/12, IPI, EU:C:2013:715, Rn. 39 und die dort angeführte Rechtsprechung.

Anwendungsbereich sollte im Hinblick auf die Zielsetzung (z. B. der Bekämpfung der Schwerkriminalität) bestimmt werden. Wenn sich eine Maßnahme generell ohne irgendeine derartige Differenzierung, Einschränkung oder Ausnahme auf alle Personen erstreckt, verstärkt das den Grundrechtseingriff[30]. Der Eingriff wird bereits verstärkt, wenn die Datenverarbeitung einen erheblichen Teil der Bevölkerung betrifft[31].

52. Der Schutz personenbezogener Daten, zu dem Artikel 8 Absatz 1 der Charta ausdrücklich verpflichtet, ist für das in ihrem Artikel 7 verankerte Recht auf Achtung des Privatlebens von besonderer Bedeutung[32]. Die Regelung muss klare und präzise Regeln für die Tragweite und Anwendung der Maßnahme vorsehen und Mindestanforderungen aufstellen, sodass die Personen, deren Daten verarbeitet wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen[33]. Das Erfordernis, über solche Garantien zu verfügen, ist umso bedeutsamer, wenn die personenbezogenen Daten automatisch verarbeitet werden und wo eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht[34]. Darüber hinaus kann eine interne oder externe (z. B. richterliche) Genehmigung des Einsatzes von Gesichtserkennungstechnologie als Garantie zum Grundrechtsschutz beitragen; in gewissen Fällen schwerer Eingriffe mag sie sich als erforderlich erweisen.[35]

53. Die Vorschriften müssen auch der spezifischen Situation angepasst werden, z. B. im Hinblick auf die verarbeitete Datenmenge, die Art der Daten[36] und die Gefahr rechtswidrigen Datenzugriffs. Dies erfordert Regeln, die insbesondere klare und strikte Vorkehrungen für den Schutz und die Sicherheit der betreffenden Daten treffen, damit deren Unversehrtheit und Vertraulichkeit in vollem Umfang gewährleistet sind[37].

54. Im Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter sollte es den Auftragsverarbeitern nicht gestattet sein, bei der Bestimmung des von ihnen angewandten Sicherheitsniveaus ausschließlich wirtschaftliche Erwägungen zu berücksichtigen, weil dann die Gefahr bestünde, dass das Schutzniveau nicht hinreichend hoch wäre[38].

55. Die materiellen und formellen Voraussetzungen sowie die objektiven Kriterien für die Bestimmung der für den Datenzugang der zuständigen Behörden und ihre spätere Datennutzung geltenden Grenzen müssen in einem Gesetz geregelt sein. Was die Zwecke der Verhütung, Feststellung oder Verfolgung von Straftaten angeht, müssen die betreffenden Straftaten im Hinblick auf das Ausmaß und die Schwere des Eingriffs in die in den Artikeln 7 und 8 der Charta verankerten Grundrechte als hinreichend schwer angesehen werden können, um einen solchen Eingriff zu rechtfertigen[39].

---

[30] EuGH – C-594/12, Rn. 57.
[31] EuGH – C-594/12, Rn. 56.
[32] EuGH – C-594/12, Rn. 53.
[33] EuGH – C-594/12, Rn. 54, mit weiteren Nachweisen: vgl. entsprechend zu Artikel 8 EMRK, EGMR, Liberty and Others v. the United Kingdom, Urteil vom 1. Juli 2008, Nr. 58243/00, Rn. 62 und 63; Rotaru v. Romania, Rn. 57 bis 59, sowie S. und Marper v. the United Kingdom, Rn. 99.
[34] EuGH – C-594/12, Rn. 55, mit weiteren Nachweisen: vgl. entsprechend zu Artikel 8 EMRK, S. and Marper v. the United Kingdom, Rn. 103 und M. K. v. France, Urteil vom 18. April 2013, Nr. 19522/09, Rn. 35.
[35] EGMR, Szabó and Vissy v. Hungary, Rn. 73-77.
[36] Vgl. auch die für die Verarbeitung besonderer Datenkategorien geltenden erhöhten Anforderungen an technische und organisatorische Maßnahmen in Artikel 29 Absatz 1 JI-Datenschutzrichtlinie.
[37] EuGH – C-594/12, Rn. 66.
[38] EuGH – C-594/12, Rn. 67.
[39] EuGH – C-594/12, Rn. 60 und 61.

56. Die Daten müssen auf solche Weise verarbeitet werden, dass Anwendbarkeit und Wirksamkeit der unionsrechtlichen Datenschutzvorschriften sichergestellt sind; dies gilt insbesondere für Artikel 8 der Charta, wonach die Einhaltung im Hinblick auf Datenschutz und Datensicherheit von einer unabhängigen Stelle überwacht wird. In diesem Zusammenhang kann der geografische Ort, an dem die Datenverarbeitung erfolgt, von Belang sein[40].

57. Hinsichtlich der verschiedenen Schritte der Verarbeitung personenbezogener Daten sollte bei den Datenkategorien nach Maßgabe ihres etwaigen Nutzens für das verfolgte Ziel oder anhand der betroffenen Personen unterschieden werden[41]. Die Festlegung der Verarbeitungsbedingungen, zum Beispiel die Festlegung der Speicherungsfrist, muss auf objektiven Kriterien beruhen, die gewährleisten, dass der Eingriff auf das absolut Notwendige beschränkt wird[42].

58. Die Bewertung der Erforderlichkeit und Verhältnismäßigkeit muss je nach der betreffenden Situation alle grundrechtsrelevanten Auswirkungen feststellen und berücksichtigen, zum Beispiel die Auswirkungen auf die Menschenwürde (Artikel 1 der Charta), die Gedanken-, Gewissens- und Religionsfreiheit (Artikel 10 der Charta), die Freiheit der Meinungsäußerung (Artikel 11 der Charta) sowie die Versammlungs- und Vereinigungsfreiheit (Artikel 12 der Charta).

59. Ein gravierender Aspekt ist auch, dass eine ohne Wissen der betroffenen Personen erfolgende systematische Datenverarbeitung geeignet ist, ein allgemeines Gefühl ständiger Überwachung zu erzeugen[43]. Dies kann Menschen von der Ausübung einiger oder sämtlicher betroffenen Grundrechte abhalten.

60. Gesetzgeber auf nationaler und Unionsebene, die die Bewertung der Erforderlichkeit und Verhältnismäßigkeit gesetzgeberischer Maßnahmen bezüglich der Gesichtserkennung im Bereich der Strafverfolgung operationalisieren wollen, könnten sich der eigens zur Erleichterung diese Aufgabe bereitgestellten Praxis-Tools bedienen. Dazu eignet sich insbesondere das vom Europäischen Datenschutzbeauftragten herausgegebene Toolkit[44] zur Beurteilung der Erforderlichkeit und Verhältnismäßigkeit.

3.1.3.5 Artikel 52 Absatz 3 und Artikel 53 der Charta (Schutzniveau, auch in Bezug auf die EMRK)

61. Gemäß Artikel 52 Absatz 3 und Artikel 53 der Charta kommt Rechten, soweit sie den durch die EMRK garantierten Rechten entsprechen, die gleiche Bedeutung und Tragweite wie in der EMRK zu. Während es insbesondere für Artikel 7 der Charta eine Entsprechung in der EMRK gibt, ist dies für Artikel 8 der Charta nicht der Fall[45]. Artikel 52 Absatz 3 der Charta steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt. Da die EMRK kein Rechtsinstrument darstellt, das formell in die Unionsrechtsordnung übernommen wurde, muss die Unionsgesetzgebung im Lichte der durch die Charta verbürgten Grundrechte erfolgen[46].

---

[40] EuGH – C-594/12, Rn. 68.
[41] EuGH – C-594/12, Rn. 63.
[42] EuGH – C-594/12, Rn. 64.
[43] EuGH – C-594/12, Rn. 37.
[44] Europäischer Datenschutzbeauftragter: Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf den Schutz personenbezogener Daten einschränken: Ein Toolkit (11.4.2017); Europäischer Datenschutzbeauftragter: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019), nur in englischer Sprache (Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken (19.12.2019)).
[45] EuGH – C-203/15 – Tele2 Sverige, Rn. 129.
[46] EuGH – C-311/18, Rn. 99.

62. Artikel 8 der EMRK bestimmt, dass eine Behörde in die Ausübung des Rechts auf Achtung des Privat- und Familienlebens nur eingreifen darf, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

63. In der EMRK sind auch Anforderungen an die Art und Weise der Grundrechtseinschränkung festgelegt. Zu den Grundanforderungen zählt neben dem rechtsstaatlichen Gesetzesvorbehalt auch die Vorhersehbarkeit. Die Anforderung an die Vorhersehbarkeit ist erfüllt, wenn das innerstaatliche Recht hinreichend klar formuliert ist, damit jede Person angemessenen Aufschluss darüber hat, unter welchen Umständen und Voraussetzungen die Behörden zu den betreffenden Maßnahmen befugt sind[47]. Diese Anforderung wird vom EuGH und im Datenschutzrecht der Union anerkannt (vgl. Abschnitt 3.2.1.1).

64. Die Bestimmungen des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[48], in denen die Rechte aus Artikel 8 EMRK näher ausgeführt werden, sind ebenfalls in vollem Umfang einzuhalten. Allerdings ist zu beachten, dass diese Bestimmungen im Hinblick auf das maßgebliche Unionsrecht lediglich die Mindestanforderungen festlegen.

3.2 Spezifischer Rechtsrahmen – die JI-Datenschutzrichtlinie

65. Die JI-Datenschutzrichtlinie setzt einen gewissen Rahmen für den Einsatz von Gesichtserkennungstechnologie. Erstens ist in Artikel 3 Nummer 13 JI-Datenschutzrichtlinie der Begriff „biometrische Daten“[49] definiert. Vgl. dazu im Einzelnen oben in Abschnitt 2.1. Zweitens wird in Artikel 8 Absatz 2 klargestellt, dass eine Verarbeitung nur rechtmäßig ist, wenn sie für die in Artikel 1 Absatz 1 der JI-Datenschutzrichtlinie genannten Ziele erforderlich und zudem in nationalem Recht geregelt ist, in welchem zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben sind. Weitere Bestimmungen von besonderer Relevanz für biometrische Daten sind die Artikel 10 und 11 der JI-Datenschutzrichtlinie. Artikel 10 ist in Verbindung mit Artikel 8 der JI-Datenschutzrichtlinie zu lesen[50]. Die in Artikel 4 der JI-Datenschutzrichtlinie niedergelegten Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten sollten stets eingehalten werden und jede Bewertung einer etwaigen Verarbeitung biometrischer Daten durch Gesichtserkennungstechnologie sollte sich an diesen Grundsätzen orientieren.

3.2.1 Verarbeitung besonderer Kategorien von Daten für Strafverfolgungszwecke

66. Gemäß Artikel 10 der JI-Datenschutzrichtlinie ist die Verarbeitung besonderer Kategorien von Daten, zum Beispiel biometrischer Daten, nur dann erlaubt, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und wenn sie darüber hinaus nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist, der

[47] Europäischer Gerichtshof für Menschenrechte, Urteil, CASE OF COPLAND v. THE UNITED KINGDOM, 03/04/2007, Antrag Nr. 62617/00, Rn. 46.

[48] SEV-Nr. 108.

[49] Artikel 3 Nummer 13 JI-Datenschutzrichtlinie lautet: „‚biometrische Daten' mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten“.

[50] Artikel-29-Datenschutzgruppe, Stellungnahme zu einigen wesentlichen Aspekten der Richtlinie zum Datenschutz bei der Strafverfolgung (EU 2016/680), S. 7.

Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat. Aus dieser Generalklausel wird die Sensibilität der Verarbeitung besonderer Kategorien von Daten deutlich.

3.2.1.1 Zulässigkeit nach Unionsrecht oder einzelstaatlichem Recht

67. Hinsichtlich der erforderlichen Art der Gesetzgebungsmaßnahme heißt es in Erwägungsgrund 33 der JI-Datenschutzrichtlinie, dass „[w]enn in dieser Richtlinie auf das Recht der Mitgliedstaaten, eine Rechtsgrundlage oder eine Gesetzgebungsmaßnahme Bezug genommen wird, … dies nicht notwendigerweise einen von einem Parlament angenommenen Gesetzgebungsakt [erfordert], wobei Anforderungen gemäß der Verfassungsordnung des betreffenden Mitgliedstaats unberührt bleiben“[51].

68. Nach Artikel 52 Absatz 1 der Charta der Grundrechte muss jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten „gesetzlich vorgesehen sein“. Damit wird die Formulierung „gesetzlich vorgesehen“ aus Artikel 8 Absatz 2 der EMRK aufgegriffen, die nicht nur zum Ausdruck bringt, dass die Beschränkung mit den einschlägigen Rechtsvorschriften in Einklang stehen muss, sondern auch, dass diese Rechtsvorschriften – unabhängig von der Art – eine bestimmte Eigenschaft aufweisen müssen: Sie müssen dem Rechtsstaatsprinzip genügen.

69. In Erwägungsgrund 33 JI-Datenschutzrichtlinie heißt es weiter, „Recht der Mitgliedstaaten, Rechtsgrundlagen oder Gesetzgebungsmaßnahmen sollten jedoch klar und präzise sein und ihre Anwendung sollte für diejenigen, die ihnen unterliegen, vorhersehbar sein, wie in der Rechtsprechung des Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte gefordert. Im Recht der Mitgliedstaaten, das die Verarbeitung personenbezogener Daten innerhalb des Anwendungsbereichs dieser Richtlinie regelt, sollten zumindest die Ziele, die zu verarbeitenden personenbezogenen Daten, die Zwecke der Verarbeitung sowie Verfahren zur Wahrung von Integrität und Vertraulichkeit der personenbezogenen Daten und Verfahren für ihre Vernichtung angegeben werden“.

70. Das innerstaatliche Recht muss hinreichend klar formuliert sein, damit die betroffenen Personen angemessen auf die Umstände und Voraussetzungen hingewiesen werden, unter denen Verantwortliche befugt sind, derartige Beschränkungen vorzunehmen. Dazu gehören ggf. die Voraussetzungen für die Verarbeitung wie etwa bestimmte Arten Beweismitteln sowie die Erforderlichkeit einer richterlichen oder internen Genehmigung. Die jeweilige Rechtsvorschrift kann in technologischer Hinsicht neutral sein, sofern die spezifischen Risiken und Charakteristika der Verarbeitung personenbezogener Daten durch Gesichtserkennungssysteme hinreichend berücksichtigt sind. Nach der JI-Datenschutzrichtlinie und der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) und des Europäischen Gerichtshofs für Menschenrechte (EGMR) ist es nämlich unbedingt erforderlich, dass Gesetzgebungsmaßnahmen, die als Rechtsgrundlage für Gesichtserkennungsmaßnahmen dienen sollen, für die betroffenen Personen vorhersehbar sind.

71. Eine Gesetzgebungsmaßnahme, mit der lediglich die Generalklausel in Artikel 10 der JI-Datenschutzrichtlinie umgesetzt wird, kann nicht als Rechtsgrundlage dafür dienen, dass biometrische Daten mittels Gesichtserkennungstechnologie zu Strafverfolgungszwecken verarbeitet werden.

72. Außer biometrischen Daten ist in Artikel 10 der JI-Datenschutzrichtlinie auch die Verarbeitung von anderen besonderen Datenkategorien geregelt, etwa von Daten, aus denen die sexuelle Orientierung,

[51] Die Art der in Betracht gezogenen Gesetzgebungsmaßnahmen muss sowohl dem Unionsrecht als auch dem nationalen Recht genügen. Je nachdem, wie schwer die Beschränkung in Grundrechte eingreift, könnte auf nationaler Ebene eine bestimmte Gesetzgebungsmaßnahme auf einer bestimmten Ebene der Normenpyramide erforderlich sein.

politische Meinung und religiöse Überzeugung hervorgehen; die Regelung erfasst also ein breites Spektrum von Verarbeitungen. In einer solchen Bestimmung, die lediglich die Generalklausel umsetzt, würden zudem die besonderen Anforderungen an die Voraussetzungen und Umstände fehlen, unter denen Strafverfolgungsbehörden zum Einsatz von Gesichtserkennungstechnologie ermächtigt wären. Wegen der Bezugnahme auf andere Arten von Daten und des ausdrücklichen Erfordernisses besonderer Garantien, die jedoch nicht im Detail geregelt sind, kann eine nationale Bestimmung, die lediglich Artikel 10 der JI-Datenschutzrichtlinie mit ähnlich allgemeinem und abstraktem Wortlaut in nationales Recht umsetzt, nicht als Rechtsgrundlage für die Verarbeitung biometrischer Daten mittels Gesichtserkennung angeführt werden, da es ihr an Bestimmtheit und Vorhersehbarkeit mangeln würde. Gemäß den Artikeln 28 Absatz 2 bzw. Artikel 46 Absatz 1 Buchstabe c der JI-Datenschutzrichtlinie sollte der Gesetzgeber, bevor er eine neue Rechtsgrundlage für jegliche Form der Verarbeitung biometrischer Daten mittels Gesichtserkennung schafft, die nationale Aufsichtsbehörde für den Datenschutz konsultieren.

3.2.1.2 Unbedingt erforderlich

73. Die Verarbeitung kann nur als „unbedingt erforderlich“ angesehen werden, wenn sich der Eingriff in das Recht auf den Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken[52]. Die Beifügung des Wortes „unbedingt“ bedeutet, dass es die Absicht des Gesetzgebers war, dass die Verarbeitung besonderer Kategorien von Daten nur unter Voraussetzungen erfolgen sollte, die noch strenger sind als die Voraussetzungen für die Erforderlichkeit (siehe oben Abschnitt 3.1.3.4). Diese Anforderung sollte als unverzichtbar verstanden werden. Sie beschränkt den Ermessensspielraum der Strafverfolgungsbehörde bei der Beurteilung der Erforderlichkeit auf das absolute Minimum. Nach der ständigen Rechtsprechung des EuGH steht die Voraussetzung der „unbedingten Erforderlichkeit“ in engem Zusammenhang mit der Anforderung, dass die Festlegung der Umstände und Voraussetzungen, unter denen die Verarbeitung erfolgen darf, auf objektive Kriterien gestützt sein muss, was jede Verarbeitung allgemeiner oder systematischer Art ausschließt[53].

3.2.1.3 Offensichtlich öffentlich gemacht

74. Was die Prüfung angeht, ob die Verarbeitung Daten betrifft, die von der betroffenen Person offensichtlich öffentlich gemacht wurden, ist daran zu erinnern, dass bei einem Foto als solchem nicht grundsätzlich anzunehmen ist, dass es sich um biometrische Daten handelt[54]. Aus dem Umstand, dass die betroffene Person ein Foto offensichtlich öffentlich gemacht hat, folgt also nicht, dass die damit verbundenen biometrischen Daten, die sich durch besondere technische Mittel dem Foto entnehmen lassen, als offensichtlich öffentlich gemacht anzusehen sind.

75. Was personenbezogene Daten im Allgemeinen angeht, so sind biometrische Daten nur dann als von der betroffenen Person offensichtlich öffentlich gemacht anzusehen, wenn die betroffene Person das biometrische Template (und nicht lediglich ein Gesichtsbild) absichtlich frei zugänglich und durch eine allgemein zugängliche Quelle öffentlich gemacht hat. Ist es ein Dritter, der biometrische Daten

[52] Ständige Rechtsprechung zum Grundrecht auf Achtung des Privatlebens, vgl. EuGH, Rechtssache C-73/07, Rn. 56 (Satakunnan Markkinapörssi und Satamedia); EuGH, Rechtssachen C-92/09 und C-93/09, Rn. 77 (Schecke und Eifert); EuGH, RechtssacheC-594/12, Rn. 52 (Digital Rights); EuGH, Rechtssache C-362/14, Rn. 92 (Schrems).

[53] EuGH Rechtssache C-623/17, Rn. 78.

[54] Vgl. Erwägungsgrund 51 DSGVO: „Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs ‚biometrische Daten‘ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.“

offenlegt, so kann nicht davon ausgegangen werden, dass die Daten von der betroffenen Person offensichtlich öffentlich gemacht wurden.

76. Überdies genügt es für die Feststellung, dass biometrische Daten offensichtlich öffentlich gemacht wurden, nicht, auf das Verhalten der betroffenen Personen abzustellen. So ist der EDSA zum Beispiel der Ansicht, dass im Falle von sozialen Netzwerken oder Online-Plattformen der Umstand, dass die betroffene Person nicht bestimmte Einstellungen zum Schutz der Privatsphäre ausgelöst oder vorgenommen hat, nicht die Annahme begründet, dass diese betroffene Person ihre personenbezogenen Daten offensichtlich öffentlich gemacht hätte und diese Daten (z. B. Fotos) ohne Zustimmung der betroffenen Person zu biometrischen Templates verarbeitet und zu Identifikationszwecken verwendet werden dürften. Allgemein ist zu sagen, dass Standardeinstellungen eines Dienstes (zum Beispiel die öffentliche Zurverfügungstellung von Templates) oder das Fehlen einer Wahlmöglichkeit (zum Beispiel die öffentliche Zurverfügungstellung von Templates, ohne dass der Nutzer diese Einstellung ändern kann) in keiner Weise so ausgelegt werden sollten, dass damit Daten offensichtlich öffentlich gemacht wurden.

3.2.2 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

77. Artikel 11 Absatz 1 der JI-Datenschutzrichtlinie bestimmt, dass die Mitgliedstaaten ein grundsätzliches Verbot ausschließlich auf einer automatischen Verarbeitung beruhender Entscheidungen (einschließlich Profiling), die eine nachteilige Rechtsfolge für die betroffene Person haben oder sie erheblich beeinträchtigen, vorsehen müssen. Als Ausnahme von diesem grundsätzlichen Verbot gilt, dass eine solche Verarbeitung möglich ist, wenn sie nach dem Unionsrecht oder mitgliedstaatlichem Recht zulässig ist, dem der Verantwortliche unterliegt und das geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen durch den Verantwortlichen. Von der Ausnahme ist restriktiver Gebrauch zu machen. Diese Voraussetzungen gelten für gewöhnliche (d. h. nicht besondere) Kategorien personenbezogener Daten. Für die Ausnahme gemäß Artikel 11 Absatz 2 der JI-Datenschutzrichtlinie gelten noch strengere Voraussetzungen und von ihr ist noch restriktiverer Gebrauch zu machen. In Absatz 2 wird hervorgehoben, dass Entscheidungen nach Absatz 1 nicht auf besonderen Kategorien personenbezogener Daten beruhen dürfen; darunter fallen insbesondere biometrische Daten zur eindeutigen Identifikation einer natürlichen Person. Eine Ausnahme kann nur vorgesehen werden, sofern geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden. Diese Ausnahme ist zusätzlich zu Artikel 10 der JI-Datenschutzrichtlinie und im Lichte der darin genannten Voraussetzungen zu lesen.

78. Je nach Gesichtserkennungssystem kann es sein, dass selbst persönliches Eingreifen zur Bewertung der von der Gesichtserkennungstechnologie gelieferten Ergebnisse für sich genommen nicht notwendigerweise hinreichende Garantie dafür bietet, dass die Rechte der Person, insbesondere das Recht auf Schutz personenbezogener Daten, geachtet werden, da ja die Verarbeitung selbst zu Verzerrungen und Fehlern führen kann. Das persönliche Eingreifen kann zudem nur dann als Garantie angesehen werden, wenn es der eingreifenden Person möglich ist, die Ergebnisse der Gesichtserkennungstechnologie im Zuge des persönlichen Eingreifens kritisch zu überprüfen. Es ist von entscheidender Bedeutung, dafür zu sorgen, dass die Person das Gesichtserkennungssystem und seine Grenzen versteht und die Ergebnisse des Systems richtig auslegen kann. Es ist auch erforderlich, dafür zu sorgen, dass Arbeitsumfeld und -organisation der Maschinengläubigkeit und ihren Auswirkungen entgegenwirken, indem man Faktoren, die eine unkritische Übernahme der Ergebnisse begünstigen (z. B. Zeitdruck, umständliche Verfahren, etwaige Karrierenachteile usw.) vermeidet.

79. Gemäß Artikel 11 Absatz 3 der JI-Datenschutzrichtlinie ist Profiling, das zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Datenkategorien wie z. B. biometrischen Daten diskriminiert werden, nach dem Unionsrecht verboten. Laut Artikel 3 Absatz 4 der JI-Datenschutzrichtlinie bezeichnet „Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Bei der Prüfung, ob geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorgesehen sind, ist zu bedenken, dass der Einsatz von Gesichtserkennungstechnologie je nachdem, wie und zu welchem Zweck er erfolgt, zu Profiling führen kann. Profiling, das zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist nach dem Unionsrecht und Artikel 11 Absatz 3 der JI-Datenschutzrichtlinie auf jeden Fall zu verbieten.

3.2.3 Kategorien betroffener Personen

80. Artikel 6 der JI-Datenschutzrichtlinie betrifft die Notwendigkeit der Unterscheidung verschiedener Kategorien betroffener Personen. Wann immer anwendbar ist diese Unterscheidung ist weitestmöglich vorzunehmen. Die Wirkung der Unterscheidung muss sich in der Art und Weise der Datenverarbeitung zeigen. Aus den in Artikel 6 der JI-Datenschutzrichtlinie gegebenen Beispielen kann geschlossen werden, dass die Verarbeitung personenbezogener Daten grundsätzlich den Kriterien der Erforderlichkeit und Verhältnismäßigkeit genügen muss, auch in Bezug auf die Kategorie betroffener Personen[55]. Des Weiteren kann daraus geschlossen werden, dass es im Falle betroffener Personen, bei denen es keine Anzeichen dafür gibt, dass ihr Verhalten eine Verbindung – und sei es auch eine nur mittelbare oder entfernte Verbindung – zum legitimen Ziel der JI-Datenschutzrichtlinie aufweisen könnte, höchstwahrscheinlich keine Rechtfertigung für einen Eingriff gibt[56]. Kommt eine Unterscheidung nach Artikel 6 der JI-Datenschutzrichtlinie nicht in Betracht oder ist sie nicht möglich, so ist die Ausnahme von der Regel in Artikel 6 der JI-Datenschutzrichtlinie bei der Beurteilung der Erforderlichkeit und Verhältnismäßigkeit des Eingriffs streng zu prüfen. Die Unterscheidung verschiedener Kategorien betroffener Personen ist, was die Verarbeitung personenbezogener Daten mittels Gesichtserkennung angeht, eine wesentliche Anforderung, zumal wenn man bedenkt, dass Falschtreffer und Falsch-Nichttreffer erhebliche Auswirkungen haben können, sowohl für die betroffenen Personen als auch für den Gang der Ermittlungen.

81. Wie bereits erwähnt, sind bei der Umsetzung von Unionsrecht die Bestimmungen der Charta der Grundrechte der Europäischen Union einzuhalten (vgl. Artikel 52 der Charta). Der Rahmen und die Kriterien, die in der JI-Datenschutzrichtlinie vorgesehen sind, sind daher im Lichte der Charta zu lesen. Rechtsakte der Union und ihrer Mitgliedstaaten dürfen nicht hinter diesen Anforderungen zurückbleiben, sondern müssen der Charta volle Wirkung verleihen.

3.2.4 Rechte der betroffenen Person

82. Der EDSA hat bereits Leitlinien zu verschiedenen Aspekten der sich aus der DSGVO ergebenden Rechte betroffener Personen herausgegeben[57]. Die JI-Datenschutzrichtlinie sieht ähnliche Rechte betroffener Personen vor, und von der Artikel-29-Datenschutzgruppe wurde bereits eine allgemeine

[55] Vgl. auch EuGH – C-594/12, Rn. 56-59.
[56] Vgl. auch EuGH – C-594/12, Rn. 58.
[57] Vgl. z. B. 1/2022 EDPB Guidelines on data subject's rights – Right of access (Leitlinien des EDSA über die Rechte betroffener Personen – Recht auf Auskunft) und Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte.

Stellungnahme dazu abgegeben, die der EDSA gebilligt hat[58]. Unter bestimmten Umständen gestattet die JI-Datenschutzrichtlinie gewisse Einschränkungen dieser Rechte. Die Voraussetzungen, unter denen solche Einschränkungen möglich sind, werden in Abschnitt 3.2.4.6 „Legitime Einschränkungen der Rechte betroffener Personen“ näher ausgeführt.

83. Alle in Kapitel III der JI-Datenschutzrichtlinie aufgeführten Rechte betroffener Personen finden natürlich auch auf die Verarbeitung personenbezogener Daten mittels Gesichtserkennungstechnologie Anwendung; im Folgenden wird jedoch auf einige Rechte und Aspekte fokussiert, hinsichtlich derer Leitlinien von besonderem Interesse sein könnten. In diesem Kapitel und der darin enthaltenen Analyse wird davon ausgegangen, dass die in Rede stehende Verarbeitung mittels Gesichtserkennungstechnologie sämtlichen im vorhergehenden Kapitel genannten rechtlichen Anforderungen genügt.

84. Wegen des Charakters der Verarbeitung personenbezogener Daten mittels Gesichtserkennungstechnologie (Verarbeitung besonderer Kategorien personenbezogener Daten, oftmals ohne ersichtliche Interaktion mit der betroffenen Person) ist sorgfältig zu prüfen, wie (oder ob) es möglich ist, die Anforderungen der JI-Datenschutzrichtlinie zu erfüllen; diese Prüfung muss stattfinden, bevor mit der Verarbeitung mittels Gesichtserkennungstechnologie begonnen wird. Dabei ist insbesondere Folgendes genau zu analysieren:

- wer die betroffenen Personen sind (häufig handelt es sich um mehr als eine Person), die im Hinblick auf den Zweck der Verarbeitung zur Zielgruppe zählen,
- wie die betroffenen Personen auf die Verarbeitung mittels Gesichtserkennungstechnologie hingewiesen werden (vgl. Abschnitt 3.2.4.1),
- wie die betroffenen Personen ihre Rechte ausüben können (hier können die Rechte auf Information und auf Auskunft sowie die Rechte auf Berichtigung oder Einschränkung beim Einsatz von Gesichtserkennungstechnologie besonders schwer aufrechtzuerhalten sein, es sei denn, es handelt sich um eine One-to-One-Verifizierung im direkten Kontakt mit der betroffenen Person).

3.2.4.1 Information und Rechtsaufklärung betroffener Personen in präziser, verständlicher und leicht zugänglicher Form

85. Beim Einsatz von Gesichtserkennungstechnologie ist die Gewährleistung der Aufklärung betroffener Personen über die Verarbeitung ihrer biometrischen Daten erschwert. Besonders schwierig ist dies, wenn eine Strafverfolgungsbehörde mittels Gesichtserkennungstechnologie Videomaterial analysiert, das von einem Dritten stammt oder geliefert wurde. In dieser Konstellation hat die Strafverfolgungsbehörde nur wenig bzw. zumeist gar keine Möglichkeit, die betroffene Person zum Zeitpunkt der Erhebung (z. B. durch Schilder am Erhebungsort) zu informieren. Alle Videoaufzeichnungen, die für die Ermittlungen (oder den Zweck der Verarbeitung) nicht relevant sind, sollten stets gelöscht oder anonymisiert werden (z. B. durch Unkenntlichmachung ohne nachträgliche Möglichkeit der Datenwiederherstellung), bevor biometrische Daten verarbeitet werden; so wird das Risiko einer Verletzung des Grundsatzes der Datenminimierung aus Artikel 4 Absatz 1 Buchstabe e der JI-Datenschutzrichtlinie und der Informationspflichten in Artikel 13 Absatz 2 der JI-Datenschutzrichtlinie vermieden. Die Verantwortung für die Beurteilung, welcher Informationen die betroffene Person für die Rechtsausübung bedarf, sowie für die Gewährleistung der Mitteilung der

[58] Artikel-29-Datenschutzgruppe, Stellungnahme zu einigen wesentlichen Aspekten der Richtlinie zum Datenschutz bei der Strafverfolgung (EU 2016/680).

erforderlichen Informationen trägt der Verantwortliche. Die wirksame Ausübung der Rechte betroffener Personen hängt davon ab, dass der Verantwortliche seine Informationspflichten erfüllt.

86. In Artikel 13 Absatz 1 der JI-Datenschutzrichtlinie sind die Mindestangaben aufgeführt, die der betroffenen Person grundsätzlich mitzuteilen sind. Diese Informationen können der betroffenen Person auf der Website des Verantwortlichen, in gedruckter Form (z. B. als auf Verlangen erhältliche Broschüre) oder in anderen leicht zugänglichen Informationsquellen mitgeteilt werden. Der Verantwortliche muss auf jeden Fall dafür Sorge tragen, dass mindestens folgende Angaben wirksam mitgeteilt werden:

- Namen und Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten,
- die Zwecke der Verarbeitung und die Art der Verarbeitung (mittels Gesichtserkennungstechnologie),
- das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde sowie deren Kontaktdaten,
- das Recht auf Auskunft sowie auf Berichtigung oder Löschung personenbezogener Daten und auf Einschränkung der Verarbeitung personenbezogener Daten.

87. In besonderen Fällen, die im nationalen Recht im Einklang mit Artikel 13 Absatz 2 der JI-Datenschutzrichtlinie[59] (z. B. für den Fall der Verarbeitung mittels Gesichtserkennungstechnologie) festgelegt werden, sind der betroffenen Person darüber hinaus folgende Informationen mitzuteilen:

- die Rechtsgrundlage der Verarbeitung,
- Angaben dazu, wo die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden,
- die Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
- gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten (auch der Empfänger in Drittländern oder internationalen Organisationen).

88. Während in Artikel 13 Absatz 1 der JI-Datenschutzrichtlinie die zur Verfügung zu stellenden allgemeinen Informationen geregelt sind, sind in Artikel 13 Absatz 2 der JI-Datenschutzrichtlinie die zusätzlichen Informationen aufgeführt, die der betroffenen Person in besonderen Fällen zu erteilen sind, wenn zum Beispiel Daten unmittelbar bei der betroffenen Person oder mittelbar ohne Wissen der betroffenen Person erhoben werden[60]. Es gibt keine eindeutige Definition des in Artikel 13 Absatz 2 der JI-Datenschutzrichtlinie verwendeten Begriffs „in besonderen Fällen“. Er bezieht sich jedenfalls auf Situationen, in denen betroffene Personen auf eine Verarbeitung, die sie persönlich betrifft, hinzuweisen und angemessen über die wirksame Ausübung ihrer Rechte zu informieren sind. Bei der Beurteilung, ob es sich um einen „besonderen Fall“ handelt, sind nach Ansicht des EDSA mehrere Faktoren zu berücksichtigen, unter anderem ob personenbezogene Daten ohne Wissen der betroffenen Person erhoben werden; schließlich ist die wirksame Ausübung ihrer Rechte den betroffenen Personen nur möglich, wenn sie davon wissen. Andere Beispiele für „besondere Fälle“ wären etwa die Weiterverarbeitung personenbezogener Daten in einem Verfahren im Rahmen der

[59] So enthält z. B. § 56 Absatz 1 des deutschen Bundesdatenschutzgesetzes unter anderem Vorgaben zu den Angaben, die betroffenen Personen im Falle verdeckter Maßnahmen mitgeteilt werden müssen.
[60] Artikel-29-Datenschutzgruppe, Stellungnahme zu einigen wesentlichen Aspekten der Richtlinie zum Datenschutz bei der Strafverfolgung (EU 2016/680), S. 17-18.

internationalen Zusammenarbeit in Strafsachen oder die Situation, dass bei verdeckten Operationen personenbezogene Daten nach den Vorgaben des nationalen Rechts verarbeitet werden. Zudem folgt aus Erwägungsgrund 38 der JI-Datenschutzrichtlinie für den Fall, dass die Entscheidungsfindung allein auf Gesichtserkennungstechnologie beruhen sollte, dass die betroffenen Personen über die Funktionsweise der automatisierten Entscheidungsfindung zu informieren sind. Auch dies würde darauf hindeuten, dass dies ein besonderer Fall im Sinne von Artikel 13 Absatz 2 der JI-Datenschutzrichtlinie ist, bei dem der betroffenen Person zusätzliche Informationen zu erteilen sind[61].

89. Abschließend ist zu beachten, dass die Mitgliedstaaten gemäß Artikel 13 Absatz 3 der JI-Datenschutzrichtlinie Gesetzgebungsmaßnahmen erlassen können, durch die die Unterrichtungspflicht in bestimmten Fällen und zu bestimmten Zwecken eingeschränkt wird. Dies gilt insoweit und so lange, wie diese Maßnahme in einer demokratischen Gesellschaft erforderlich und verhältnismäßig ist und sofern den Grundrechten und den berechtigten Interessen der betroffenen Person Rechnung getragen wird.

3.2.4.2 Recht auf Auskunft

90. Grundsätzlich hat die betroffene Person das Recht auf Bestätigung, ob ihre personenbezogenen Daten verarbeitet werden oder nicht; werden ihre Daten verarbeitet, so hat sie das Recht, Auskunft über die betreffenden personenbezogenen Daten sowie darüber hinaus die in Artikel 14 der JI-Datenschutzrichtlinie aufgeführten Informationen zu erhalten. Bei Gesichtserkennungstechnologie, die biometrische Daten speichert und auch mittels alphanumerischer Daten mit einer Identität verknüpft, sollte es der zuständigen Behörde möglich sein, das Auskunftsverlangen auf Grundlage einer Suche nach den betreffenden alphanumerischen Daten zu beantworten, ohne eine weitere Verarbeitung biometrischer Daten anderer Personen zu starten (d. h. durch eine mit Gesichtserkennungstechnologie vorgenommene Datenbanksuche). Nach dem zu beachtenden Grundsatz der Datenminimierung dürfen nicht mehr Daten gespeichert werden, als für die Zwecke der Verarbeitung erforderlich.

3.2.4.3 Recht auf Berichtigung personenbezogener Daten

91. Da Gesichtserkennungstechnologie keine absolute Richtigkeit bietet, ist es besonders wichtig, dass die Verantwortlichen bei Anträgen auf Berichtigung personenbezogener Daten wachsam sind. Es kann auch vorkommen, dass eine betroffene Person auf Grundlage der Gesichtserkennungstechnologie einer falschen Kategorie zugeordnet wird, indem sie zum Beispiel in einer auf Videoaufzeichnungen beruhenden Ersteinschätzung zur Vorgehensweise fälschlich in die Kategorie der Verdächtigen eingeordnet wird. Besonders gravierende Risiken für betroffene Personen ergeben sich, wenn unrichtige Daten in einer polizeilichen Datenbank gespeichert und/oder mit anderen Stellen ausgetauscht werden. Der Verantwortliche muss die gespeicherten Daten und Gesichtserkennungssysteme erforderlichenfalls berichtigen (vgl. Erwägungsgrund 47 der JI-Datenschutzrichtlinie).

3.2.4.4 Recht auf Löschung

92. Der Einsatz von Gesichtserkennungstechnologie wird in den meisten Fällen – soweit es sich nicht um One-to-One-Verifizierung/Authentifikation handelt – mit der Verarbeitung biometrischer Daten einer großen Zahl betroffener Personen einhergehen. Es ist deshalb wichtig, dass der Verantwortliche die

[61] Man beachte den Unterschied zwischen „der betroffenen Person zur Verfügung zu stellende“ in Artikel 13 Absatz 1 der JI-Datenschutzrichtlinie und „der betroffenen Person … erteilt“ in Artikel 13 Absatz 2 der JI-Datenschutzrichtlinie. Artikel 13 Absatz 2 der JI-Datenschutzrichtlinie erfordert, dass der Verantwortliche sicherstellt, dass die Informationen die betroffene Person erreichen; die Veröffentlichung der Informationen auf einer Website genügt nicht.

Grenzen im Hinblick auf Zweck und Erforderlichkeit vorab berücksichtigt, damit Anträge auf Löschung gemäß Artikel 16 der JI-Datenschutzrichtlinie unverzüglich bearbeitet werden können (unter anderem wenn der Verantwortliche personenbezogene Daten löschen muss, weil die Verarbeitung gegen die nach den Artikeln 4, 8 und 10 der JI-Datenschutzrichtlinie erlassenen einschlägigen Vorschriften verstößt).

3.2.4.5 Recht auf Einschränkung

93. Wenn die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann (oder wenn die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden müssen), ist der Verantwortliche verpflichtet, die Verarbeitung der personenbezogenen Daten gemäß Artikel 16 der JI-Datenschutzrichtlinie einzuschränken. Besondere Bedeutung kommt dem zu, wenn Gesichtserkennungstechnologie (die auf einem oder mehreren Algorithmen beruht und deshalb niemals ein definitives Ergebnis liefert) in Situationen eingesetzt wird, in denen große Datenmengen erhoben werden, bei denen die Richtigkeit und Qualität der Identifizierung schwanken kann. Je schlechter die Qualität der Videoaufzeichnungen (z. B. von einem Tatort), desto größer die Gefahr von Falschtreffern. Auch wenn Gesichtsbilder in einer Fahndungsliste nicht regelmäßig aktualisiert werden, steigt die Gefahr von Falschtreffern oder Falsch-Nichttreffern. Sollte im Einzelfall die Datenlöschung nicht möglich sein, weil berechtigter Grund zu der Annahme besteht, dass eine Löschung die berechtigten Interessen der betroffenen Person beeinträchtigen könnte, so sollte die Datenverarbeitung eingeschränkt werden und die Daten sollten nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand (vgl. Erwägungsgrund 47 der JI-Datenschutzrichtlinie).

3.2.4.6 Legitime Einschränkungen der Rechte betroffener Personen

94. Einschränkungen der Informationspflichten des Verantwortlichen und des Rechts betroffener Personen auf Auskunft sind nur möglich, wenn sie in einem Gesetz vorgesehen sind, welches seinerseits eine in einer demokratischen Gesellschaft erforderliche und verhältnismäßige Maßnahme darstellt, die den Grundrechten und den berechtigten Interessen der betroffenen natürlichen Person Rechnung trägt (vgl. Artikel 13 Absatz 3, Artikel 13 Absatz 4, Artikel 15 Absatz 3 und Artikel 16 Absatz 4 der JI-Datenschutzrichtlinie). Beim Einsatz von Gesichtserkennungstechnologie für Strafverfolgungszwecke ist zu erwarten, dass dieser unter Umständen erfolgt, in denen es dem verfolgten Zweck zuwiderliefe, die betroffene Person zu informieren oder ihr Auskunft über die Daten zu geben, etwa bei polizeilichen Ermittlungen in Strafsachen oder zum Schutz der nationalen oder öffentlichen Sicherheit.

95. Das Recht auf Auskunft bedeutet nicht automatisch den Zugang zu sämtlichen Informationen z. B. eines Strafverfahrens, in dem die eigenen personenbezogenen Daten erwähnt sind. Ein taugliches Beispiel für einen Fall, in dem Einschränkungen dieses Rechts gestattet sein können, sind etwa laufende strafrechtliche Ermittlungen.

3.2.4.7 Rechtsausübung durch die Aufsichtsbehörde

96. In Fällen, in denen es legitime Einschränkungen der Ausübung von Rechten gemäß Kapitel III der JI-Datenschutzrichtlinie gibt, kann die betroffene Person verlangen, dass die Datenschutzaufsichtsbehörde die Rechte der betroffenen Person in deren Namen ausübt, indem die Behörde die Rechtmäßigkeit der vom Verantwortlichen vorgenommenen Verarbeitung überprüft. Es ist Sache des Verantwortlichen, die betroffene Person über die Möglichkeit, ihre Rechte auf diese Weise auszuüben, zu informieren (vgl. Artikel 17 der JI-Datenschutzrichtlinie und Artikel 46 Absatz 1 Buchstabe g der JI-Datenschutzrichtlinie). In Bezug auf Gesichtserkennungstechnologie bedeutet das, dass der Verantwortliche sicherstellen muss, dass geeignete Maßnahmen getroffen werden, damit einem solchen Verlangen entsprochen werden kann, z. B. durch Ermöglichung der Suche nach

Aufzeichnungen; Voraussetzung ist allerdings, dass die betroffene Person hinreichende Angaben macht, anhand derer ihre personenbezogenen Daten gefunden werden können.

3.2.5 Sonstige rechtliche Anforderungen und Garantien

3.2.5.1 Artikel 27 Datenschutz-Folgenabschätzung

97. Es ist zwingend vorgeschrieben, vor Einsatz von Gesichtserkennungstechnologie eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen, da die Art der Verarbeitung, insbesondere der Einsatz neuer Technologien, im Hinblick auf Art, Umfang, Kontext und Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Da der Einsatz von Gesichtserkennungstechnologie mit systematischer automatischer Verarbeitung besonderer Kategorien von Daten verbunden ist, könnte man annehmen, dass der Verantwortliche in solchen Fällen grundsätzlich gehalten wäre, eine DSFA durchzuführen. Die DSFA sollte zumindest Folgendes enthalten: eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge, eine zweckbezogene Prüfung der Erforderlichkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge, eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken und der geplanten Risiko-Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Richtlinieneinhaltung nachgewiesen wird. Der EDSA empfiehlt als vertrauens- und transparenzsteigernde Maßnahme, die Ergebnisse solcher DSFA oder zumindest deren wichtigste Erkenntnisse und Schlussfolgerungen zu veröffentlichen[62].

3.2.5.2 Artikel 28 Vorherige Konsultation der Aufsichtsbehörde

98. Gemäß Artikel 28 der JI-Datenschutzrichtlinie muss der Verantwortliche oder der Auftragsverarbeiter vor der Verarbeitung die Aufsichtsbehörde konsultieren, wenn: a) aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft; oder b) die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat. Wie bereits in Abschnitt 2.3 dieser Leitlinien erklärt wurde, ist der EDSA der Auffassung, dass in den meisten Fällen dem Einsatz und der Verwendung von Gesichtserkennungstechnologie ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen innewohnt. Eine Behörde, die Gesichtserkennungstechnologie einsetzen will, sollte also vor dem Einsatz des Systems nicht nur die DSFA durchführen, sondern auch die zuständige Aufsichtsbehörde konsultieren.

3.2.5.3 Artikel 29 Sicherheit der Verarbeitung

99. Wegen des einzigartigen Charakters biometrischer Daten ist es einer betroffenen Person nicht möglich, diese zu ändern, falls deren Sicherheit (z. B. infolge einer Datenschutzverletzung) beeinträchtigt sein sollte. Behörden, die Gesichtserkennungstechnologie implementieren und/oder verwenden, sollten deshalb besonders auf die in Artikel 29 der JI-Datenschutzrichtlinie vorgeschriebene Sicherheit der Verarbeitung achten. Strafverfolgungsbehörden sollten insbesondere sicherstellen, dass das System den einschlägigen Normen genügt und Maßnahmen zum Schutz biometrischer Templates implementiert sind[63]. Diese Verpflichtung ist von umso größerer Bedeutung, wenn sich die Strafverfolgungsbehörde eines externen Anbieters (Auftragsverarbeiters) bedient.

---

[62] Nähere Information dazu vgl. Artikel-29-Datenschutzgruppe, WP 248 Rev. 01), Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt".

[63] Siehe beispielsweise: ISO/IEC 24745 Informationssicherheit, Cybersicherheit und Datenschutz – Schutz biometrischer Informationen.

3.2.5.4 Artikel 20 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

100. Ziel des in Artikel 20 der JI-Datenschutzrichtlinie vorgesehenen Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen ist es, die Datenschutzgrundsätze und Garantien (etwa die Grundsätze der Datenminimierung und Speicherbegrenzung) durch geeignete technische und organisatorische Maßnahmen wie die Pseudonymisierung in die Technologie einzubetten, und zwar schon vor Beginn und für die gesamte Dauer der Verarbeitung personenbezogener Daten. Wegen des inhärenten hohen Risikos für die Rechte und Freiheiten natürlicher Personen sollte die Auswahl derartiger Maßnahmen nicht allein von wirtschaftlichen Erwägungen abhängig gemacht werden[64]; vielmehr sollte angestrebt werden, dem Stand der Technik entsprechende Datenschutztechnologie zu implementieren. Gleichermaßen sollte eine Strafverfolgungsbehörde, die Gesichtserkennungstechnologie externer Anbieter anwenden und benutzen will, sicherstellen (z. B. im Vergabeverfahren), dass ausschließlich Gesichtserkennungstechnologie, die auf den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen aufbaut, zum Einsatz kommt[65]. Das bedeutet auch, dass die Transparenz über die Funktionsweise der Gesichtserkennungstechnologie nicht durch Geltendmachung von Geschäftsgeheimnissen oder Rechten des geistigen Eigentums eingeschränkt wird.

3.2.5.5 Artikel 25 Protokollierung

101. Die JI-Datenschutzrichtlinie sieht verschiedene Methoden vor, nach denen der Verantwortliche oder der Auftragsverarbeiter die Rechtmäßigkeit der Verarbeitung nachweisen und die Datenintegrität und Datensicherheit sicherstellen kann. Dabei sind Systemprotokolle ein sehr nützliches Mittel und eine wichtige Garantie für die Überprüfung der Rechtmäßigkeit der Verarbeitung, die intern (d. h. durch Eigenüberwachung) bzw. extern durch Aufsichtsbehörden wie etwa die Datenschutzaufsichtsbehörden durchgeführt wird. Gemäß Artikel 25 der JI-Datenschutzrichtlinie sind in Systemen für die automatisierte Verarbeitung zumindest die folgenden Verarbeitungsvorgänge zu protokollieren: Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung. Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identifizierung der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers solcher personenbezogenen Daten festzustellen. Im Zusammenhang mit Gesichtserkennungssystemen wird zudem empfohlen, die folgenden zusätzlichen Verarbeitungsvorgänge zu protokollieren (zum Teil über Artikel 25 der JI-Datenschutzrichtlinie hinausgehend):

- Änderungen der Referenzdatenbank (Hinzufügung, Löschung oder Aktualisierung): Ist die Rechtmäßigkeit oder das Ergebnis der Verarbeitungsvorgänge nicht anders überprüfbar, sollte das Protokoll eine Kopie des betreffenden (hinzufügten, gelöschten oder aktualisierten) Bilds enthalten.

- Identifikations- oder Verifizierungsversuche einschließlich Ergebnis und Konfidenz-Score: Der Grundsatz der Datenminimierung sollte streng eingehalten werden, sodass nur der Identifikator des Bildes aus der Referenzdatenbank und nicht das Referenzbild in den Protokollen gespeichert

[64] Siehe Erwägungsgrund 53 der JI-Datenschutzrichtlinie.

[65] Weitere Informationen dazu siehe Leitlinien des EDSA zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf) .

wird. Die Protokollierung der eingegebenen biometrischen Daten sollte vermieden werden, es sei denn, sie ist (z. B. bei Treffern) erforderlich.

- Die Identität des Nutzers, der den Identifikations- oder Verifizierungsversuch gemacht hat.

- Jegliche Speicherung personenbezogener Daten in den Systemprotokollen unterliegt der strengen Zweckbindung (z. B. Audits) und sollte für keine anderen Zwecke genutzt werden (etwa um weiterhin Erkennungen/Verifizierungen anhand eines bereits aus der Referenzdatenbank gelöschten Bildes durchführen zu können). Es sind Sicherheitsmaßnahmen anzuwenden, um die Integrität der Protokolle sicherzustellen, wobei automatische Überwachungssysteme zur Aufdeckung missbräuchlicher Protokollnutzung dringend empfohlen werden. Im Falle der Speicherung von Gesichtsbildern sollten die Sicherheitsmaßnahmen für die Referenzdatenbankprotokolle denen für die Referenzdatenbank gleichwertig sein. Außerdem sollten automatische Verfahren implementiert werden, um die Einhaltung der Datenspeicherfristen für die Protokolle sicherzustellen.

3.2.5.6 Artikel 4 Absatz 4 Rechenschaftspflicht

102. Gemäß Artikel 4 Absatz 4 der JI-Datenschutzrichtlinie muss der Verantwortliche die Einhaltung der in Artikel 4 Absätze 1 bis 3 genannten Grundsätze nachweisen können. Dafür unerlässlich sind eine systematische und aktuelle Systemdokumentation (einschließlich Updates, Upgrades und algorithmisches Training), technische und organisatorische Maßnahmen (einschließlich Überwachung der Systemleistung und potenzielles persönliches Eingreifen) sowie die Verarbeitung personenbezogener Daten. Ein besonders wichtiges Element für den Nachweis der Rechtmäßigkeit der Verarbeitung ist die Protokollierung gemäß Artikel 25 der JI-Datenschutzrichtlinie (vgl. Abschnitt 3.2.5.5). Der Grundsatz der Rechenschaftspflicht bezieht sich nicht nur auf das System und die Verarbeitung, sondern auch auf die Dokumentation der Verfahrensgarantien, z. B. Prüfungen der Erforderlichkeit und Verhältnismäßigkeit, DSFA wie auch interne Konsultationen (z. B. Genehmigung des Projekts durch Vorgesetzte oder interne Entscheidungen über die Werte für den Konfidenz-Score) und externe Konsultationen (z. B. Datenschutzbehörde (DSB)). In Anhang II sind einige dieser Elemente aufgeführt.

3.2.5.7 Artikel 47 Wirksame Aufsicht

103. Die wirksame Aufsicht durch die zuständigen Datenschutzbehörden ist eine der wichtigsten Garantien für die Grundrechte und Freiheiten der vom Einsatz von Gesichtserkennungstechnologie betroffenen Personen. Dabei ist die Ausstattung jeder Datenschutzbehörde mit den erforderlichen personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen Voraussetzung dafür, dass diese ihre Aufgaben und Befugnisse effektiv wahrnehmen kann[66]. Noch wichtiger als die Zahl der verfügbaren Mitarbeiter sind die Fähigkeiten der Experten, die ein sehr breites Spektrum von Fachgebieten abdecken sollten – von strafrechtlichen Ermittlungen und polizeilicher Zusammenarbeit bis hin zu Big-Data-Analyse und KI. Die Mitgliedstaaten sollten deshalb sicherstellen, dass die Aufsichtsbehörden mit geeigneten und ausreichenden Mitteln ausgestattet sind, um ihre Aufgabe – den Schutz der Rechte betroffener Personen – wahrnehmen und alle diesbezüglichen Entwicklungen genau verfolgen zu können[67].

[66] Vgl. Mitteilung der Kommission, „Erster Bericht über die Anwendung und Wirkungsweise der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung)“, COM(2022) 364 final, Abschnitt 3.4.1.

[67] Vgl. Contribution of the EDPB to the European Commission’s evaluation of the Data Protection Law Enforcement Directive (LED) (Beitrag des EDSA zu der von der Europäischen Kommission durchgeführten Evaluierung der Richtlinie zum Datenschutz bei der Strafverfolgung), Artikel 62 Rn. 14, https://edpb.europa.eu/system/files/2021-12/edpb_contribution_led_review_en.pdf.

4 SCHLUSSFOLGERUNG

104. Der Einsatz von Gesichtserkennungstechnologien geht notwendigerweise mit der Verarbeitung erheblicher Mengen personenbezogener Daten einher; dabei werden auch besondere Datenkategorien verarbeitet. Das Gesicht wie auch, allgemein gesprochen, biometrische Daten haben einen dauerhaften und unwiderruflichen Bezug zur Identität einer Person. Die Verwendung von Gesichtserkennung hat deshalb unmittelbare oder mittelbare Auswirkungen auf zahlreiche der in der EU-Charta der Grundrechte verankerten Grundrechte und Freiheiten, nicht nur auf den Schutz der Privatsphäre und den Datenschutz, sondern auch auf die Menschenwürde, die Freizügigkeit, die Versammlungsfreiheit und andere mehr. Besonders relevant ist dies im Bereich der Strafverfolgung und Strafjustiz.

105. Der EDSA hat Verständnis dafür, dass es für Gefahrenabwehr- und Strafverfolgungsbehörden wichtig ist, über die bestmöglichen Instrumente für eine rasche Identifizierung von Terroristen oder anderen Schwerkriminellen zu verfügen. Derartige Instrumente müssen jedoch unter strikter Einhaltung des einschlägigen Rechtsrahmens und ausschließlich in solchen Fällen verwendet werden, in denen die in Artikel 52 Absatz 1 der Charta niedergelegten Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit erfüllt sind. Moderne Technologien mögen Teil der Lösung sein, sie sind aber keinesfalls eine Universallösung.

106. Es gibt einige Anwendungsmöglichkeiten von Gesichtserkennungstechnologie, die inakzeptabel hohe Risiken für die Menschen und die Gesellschaft darstellen („rote Linien“). Deshalb fordern der EDSA und der EDSB, solche Anwendungen allgemein zu verbieten[68].

107. Insbesondere für die biometrische Fernidentifizierung natürlicher Personen in frei zugänglichen öffentlichen Räumen, die ein hohes Risiko des Eingriffs in die Privatsphäre natürlicher Personen darstellt, ist in einer demokratischen Gesellschaft kein Raum, denn dabei handelt es sich um eine Massenüberwachung. Gleichermaßen hält der EDSA KI-gestützte Gesichtserkennungssysteme, die natürliche Personen nach biometrischen Merkmalen (etwa nach ethnischer Zugehörigkeit, Geschlecht bzw. politischer oder sexueller Orientierung) in Cluster eingruppieren, für nicht mit der Charta vereinbar. Auch der Einsatz von Gesichtserkennung oder ähnlichen Technologien zur Erkennung der Emotionen natürlicher Personen ist nach Ansicht des EDSA höchst unerwünscht und sollte – möglicherweise mit einigen wenigen, gut begründeten Ausnahmen – verboten werden. Im Bereich der Strafverfolgung würde eine Verarbeitung personenbezogener Daten, die auf einer Datenbank personenbezogener Daten beruhte, die z. B. durch massenhaftes und unterschiedsloses Auslesen („Scrapen“) online, insbesondere in sozialen Netzwerken, zugänglicher Fotos und Gesichtsbildnisse erstellt wurden, nach Ansicht des EDSA den strengen Erforderlichkeitsanforderungen des Unionsrechts nicht genügen.

5 ANHÄNGE

Anhang I: Vorlage

[68] Gemeinsame Stellungnahme 5/2021 des EDSA und EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz)https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

Anhang II: Praxisleitfaden für die Projektleitung beim Einsatz von Gesichtserkennungstechnologie durch Strafverfolgungsbehörden

Anhang III: Praktische Beispiele

ANHANG I – VORLAGE FÜR DIE SZENARIOBESCHREIBUNG

(Mit Infokästen zu den für das Szenario relevanten Aspekten)

Beschreibung der Verarbeitung:

- Beschreibung der Verarbeitung, Kontext (Straftatbezug), Zweck

Informationsquelle:

- Arten betroffener Personen: ☐ alle Bürger ☐ verurteilte Straftäter ☐ Verdächtige
  ☐ Kinder ☐ andere vulnerable betroffene Personen
- Bildquelle: ☐ frei zugängliche öffentliche Räume ☐ Internet
  ☐ private Einrichtung ☐ andere natürliche Personen
  ☐ sonstige .....
- Bezug zur Straftat: ☐ unmittelbarer zeitlicher Bezug
  ☐ kein unmittelbarer zeitlicher Bezug
  ☐ unmittelbarer räumlicher Bezug
  ☐ kein unmittelbarer räumlicher Bezug

  ☐ Nicht erforderlich
- Art der Informationserfassung: ☐ aus der Ferne
  ☐ in einer Kabine oder in kontrollierter Umgebung
- Kontext – Eingriff in andere Grundrechte:
  ☐ Nein
  Ja, nämlich ☐ Versammlungsfreiheit
  ☐ Meinungsäußerungsfreiheit
  ☐ Verschiedene:.....
- Etwaige zusätzliche Informationsquellen bezüglich der betroffenen Person:
  ☐ Identitätsausweis
  ☐ Nutzung des öffentlichen Telefonnetzes
  ☐ Kfz-Kennzeichen
  ☐ Sonstige .....

Referenzdatenbank (für den Abgleich der erfassten Informationen):

- Spezifizität: ☐ Allgemeinzweckdatenbanken
  ☐ besondere Datenbanken für den Kriminalitätsbereich
- Angaben dazu, wie (und auf welcher Rechtsgrundlage) die Referenzdatenbanken populiert wurden
- Zweckänderung der Datenbank (z. B. Primärziel war Schutz von Privateigentum): ☐ JA
  ☐ NEIN

Algorithmus:

- Art der Verarbeitung: ☐ One-to-One-Verifizierung (Authentifikation)
  ☐ One-to-Many-Identifikation
- Erwägungen im Hinblick auf die Richtigkeit

- Technische Garantien

Ergebnis:

- Auswirkungen

  ☐ Unmittelbare Auswirkungen (z. B. Festnahme, Befragung der betroffenen Personen; diskriminierendes Verhalten)

  ☐ keine unmittelbaren Auswirkungen (Verwendung für statistische Modelle, keine gravierenden rechtlichen Maßnahmen gegen betroffene Personen)

- Automatisierte Entscheidung: ☐ JA ☐ NEIN
- Speicherfrist

Rechtliche Prüfung:

- Prüfung der Erforderlichkeit und Verhältnismäßigkeit – Zweck/Schwere der Straftat / Zahl der von der Verarbeitung betroffenen Personen, die nicht an Straftaten beteiligt sind
- Art der Vorabinformation der betroffenen Person:

  ☐ Bei Betreten des betreffenden Bereichs

  ☐ Allgemeine Informationen auf der Website der Strafverfolgungsbehörde

  ☐ Auf der Website der Strafverfolgungsbehörde für die betreffende Verarbeitung

  ☐ Sonstige .....
- Einschlägiger rechtlicher Rahmen:

  ☐ JI-Datenschutzrichtlinie größtenteils wortgleich ins nationale Recht übernommen

  ☐ Allgemeine nationale Rechtsvorschriften für die Verwendung biometrischer Daten durch Strafverfolgungsbehörden

  ☐ Besondere nationale Rechtsvorschriften für die Verarbeitung (Gesichtserkennung) durch diese zuständige Behörde

  ☐ Besondere nationale Rechtsvorschriften für diese Verarbeitung (automatisierte Entscheidung)

Ergebnis:

Allgemeine Erwägungen dazu, ob die beschriebene Verarbeitung wahrscheinlich mit dem Unionsrecht vereinbar sein dürfte (mit kurzen Angaben zu den rechtlichen Voraussetzungen)

ANHANG II – PRAXISLEITFADEN FÜR DIE PROJEKTLEITUNG BEIM EINSATZ VON GESICHTSERKENNUNGSTECHNOLOGIE DURCH STRAFVERFOLGUNGSBEHÖRDEN

Dieser Anhang enthält einen zusätzlichen Praxisleitfaden für Strafverfolgungsbehörden, die ein Projekt, bei dem Gesichtserkennungstechnologie zum Einsatz kommen soll, zu planen beginnen. Der Leitfaden bietet weitere Informationen über organisatorische und technische Maßnahmen, die im Rahmen des Projekts bedacht werden sollten; er ist jedoch nicht als erschöpfende Auflistung aller erforderlichen Prozessschritte/Maßnahmen anzusehen. Zudem sollte er in Verbindung mit den vom EDSA herausgegebenen Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte[69] sowie den einschlägigen Verordnungen auf EU/EWR-Ebene und den Leitlinien des EDSA über die Verwendung künstlicher Intelligenz gelesen werden.

Die Leitlinien in diesem Anhang beruhen auf der Annahme, dass die Gesichtserkennungstechnologie von den Strafverfolgungsbehörden beschafft wird (als direkt einsetzbares Fertigprodukt). Sollte die Strafverfolgungsbehörde planen, die Gesichtserkennungstechnologie weiterzuentwickeln (weiter zu trainieren), so gelten für die Auswahl der erforderlichen Trainings-, Validierungs- und Testdatensätze, die für die Weiterentwicklung eingesetzt werden, sowie für die Rollen/Maßnahmen in der Entwicklungsumgebung zusätzliche Anforderungen. Gleichermaßen mag es sein, dass das Fertigprodukt der Anpassung bedarf, um es für den beabsichtigten Zweck zu verwenden; auch in solchen Fällen sind die vorgenannten Anforderungen an die Auswahl der erforderlichen Test-, Validierungs- und Trainingsdatensätze zu erfüllen.

Die Zugehörigkeit zur selben Strafverfolgungsbehörde begründet für sich allein noch nicht den vollen Zugang zu biometrischen Daten. Genauso wie andere Kategorien personenbezogener Daten auch dürfen biometrische Daten, die aufgrund einer bestimmten Rechtsgrundlage zu bestimmten Strafverfolgungszwecken erhoben wurden, nicht ohne geeignete Rechtsgrundlage für einen anderen Strafverfolgungszweck verwendet werden (Artikel 4 Absatz 2 der Richtlinie (EU) 2016/680 (JI-Datenschutzrichtlinie)). Auch das Entwickeln/Trainieren von Tools für die Gesichtserkennung stellt einen anderen Zweck dar. Wenn es also darum geht, die Leistungsfähigkeit der Technologie zu messen bzw. das Tool zu trainieren, um sich aus geringer Leistungsfähigkeit ergebende Auswirkungen auf betroffene Personen zu vermeiden, ist deshalb zu prüfen, ob die mit der Messung/dem Trainieren verbundene Verarbeitung biometrischer Daten im Hinblick auf den ursprünglichen Verarbeitungszweck erforderlich und verhältnismäßig ist.

1. ROLLEN UND ZUSTÄNDIGKEITEN

Setzt eine Strafverfolgungsbehörde für die Wahrnehmung ihrer unter die JI-Datenschutzrichtlinie fallenden Aufgaben (Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten usw. im Sinne von Artikel 3 der JI-Datenschutzrichtlinie) Gesichtserkennungstechnologie ein, so kann sie als der für die Gesichtserkennungstechnologie Verantwortliche angesehen werden. Strafverfolgungsbehörden bestehen jedoch aus mehreren Referaten/Abteilungen, die unter Umständen bei dieser Verarbeitung mitwirken, sei es, indem sie das Verfahren für die Anwendung der Gesichtserkennungstechnologie festlegen oder indem sie diese in der Praxis anwenden. Wegen der Besonderheiten dieser Technologie

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

kann es sein, dass mehrere Referate daran mitwirken müssen, die Leistungsfähigkeit der Technologie zu messen oder die Technologie weiter zu trainieren.

An einem Projekt, für das Gesichtserkennungstechnologie eingesetzt wird, müssen unter Umständen verschiedene Stellen[70] innerhalb der Strafverfolgungsbehörde mitwirken:

- Oberste Leitung – zuständig für die Projektgenehmigung nach Risiko-Nutzen-Abwägung.
- Datenschutzbeauftragter und/oder Rechtsabteilung der Strafverfolgungsbehörde – unterstützt die Beurteilung der Rechtmäßigkeit der Implementierung eines bestimmten Gesichtserkennungsprojekts; unterstützt die Durchführung der DSFA; gewährleistet die Wahrung und Ausübung der Rechte der betroffenen Personen.
- Prozesseigner – fungiert innerhalb der zuständigen Strafverfolgungsbehörde als die für die Entwicklung des Gesichtserkennungsprojekts und die Entscheidung über die Details des Gesichtserkennungsprojekts (einschließlich der Anforderungen an die Systemleistung) zuständige Stelle; entscheidet über geeignete Fairness-Metrik; legt den Konfidenz-Score[71] fest; setzt akzeptable Schwellenwerte für Bias; identifiziert potenzielle Risiken des Gesichtserkennungsprojekts im Hinblick auf die Rechte und Freiheiten natürlicher Personen (durch Konsultation des Datenschutzbeauftragten und der Abteilung für IT, KI und/oder Datenwissenschaft (siehe unten)) und legt diese der obersten Leitung vor. Bevor der Prozesseigner über die Einzelheiten des Gesichtserkennungsprojekts entscheidet, konsultiert er auch den Verwalter der Referenzdatenbank, um sowohl den Verwendungszweck der Referenzdatenbank als auch deren technischen Einzelheiten zu verstehen. Wird eine beschaffte Gesichtserkennungstechnologie neu trainiert, so ist der Prozesseigner auch für die Auswahl des Trainingsdatensatzes zuständig. Da der Prozesseigner die Stelle ist, die mit der Entwicklung und den Detailentscheidungen über das Projekts betraut ist, ist er auch für die Durchführung der DSFA zuständig.
- Abteilung für IT, KI und/oder Datenwissenschaft – unterstützt die Durchführung der DSFA; erklärt die für die Messung von Systemleistung, Fairness[72] und potenziellem Bias verfügbaren Metriken; implementiert die Technologie und die technischen Garantien, um den unbefugten Zugang zu erhobenen Daten, Cyberangriffe usw. zu verhindern. Wird beschaffte Gesichtserkennungstechnologie neu trainiert, so wird das System von der Abteilung für IT, KI oder Datenwissenschaft auf Grundlage des vom Prozesseigner gestellten Trainingsdatensatzes trainiert. Diese Abteilung ist auch verantwortlich für die Festlegung der Maßnahmen zur Minderung der von den Prozesseignern gemeinsam identifizierten Risiken (z. B. KI-spezifische Risiken wie Model Inference Attacks (MIAs)).
- Endnutzer (etwa Polizeibeamte im Einsatz oder in forensischen Labors) – nehmen den Datenbankabgleich vor; unterziehen die Ergebnisse einer kritischen Prüfung, unter

[70] Die folgenden Rollen zeigen, welche verschiedenen Stellen in Betracht kommen und wo deren Verantwortlichkeiten für ein Gesichtserkennungsprojekt liegen. Die Strafverfolgungsbehörden brauchen der hier verwendeten Terminologie nicht zu folgen, sie müssen jedoch entsprechend ihrer Organisation vergleichbare Rollen festlegen und zuweisen. Eine Stelle kann auch mehr als eine Rolle übernehmen, indem sie zum Beispiel sowohl als Prozesseigner als auch als Verwalter der Referenzdatenbank fungiert, oder aber als Prozesseigner und als Abteilung für IT, KI und/oder Datenwissenschaft (sofern die Stelle, die als Prozesseigner fungiert, über das erforderliche technische Fachwissen verfügt).

[71] Der Konfidenz-Score bezeichnet das Konfidenzniveau der Vorhersage (Treffer) in Form eines Wahrscheinlichkeitswerts, dass z. B. die Konfidenz beim Abgleich zweier Templates, dass diese zur selben Person gehören, 90 % beträgt. Der Konfidenz-Score ist etwas anderes als die Leistungsfähigkeit der Gesichtserkennungstechnologie, er hat aber Einfluss auf die Leistungsfähigkeit. Je höher die Konfidenzschwelle, desto geringer die Zahl der Falschtreffer und desto höher die Zahl der Falsch-Nichttreffer unter den Ergebnissen der Gesichtserkennungstechnologie.

[72] Fairness kann als Freiheit von unfairer, rechtswidriger Diskriminierung (wie Verzerrungen (Bias) im Hinblick auf Geschlecht oder Rasse) definiert werden.

Berücksichtigung vorhandener Beweise, und geben dem Prozesseigner Feedback zu Falschtreffern sowie Hinweise auf etwaige Diskriminierung.

- Verwalter der Referenzdatenbank – die spezifische Stelle innerhalb der Strafverfolgungsbehörde, die für Aufbau und Verwaltung der Referenzdatenbank (d. h. die Datenbank, mit der der Bildabgleich erfolgt) zuständig ist, was auch die Löschung von Gesichtsbildern bei Ablauf der festgelegten Speicherfrist einschließt. Eine solche Datenbank kann eigens für das vorgesehene Gesichtserkennungsprojekt eingerichtet werden oder bereits für damit kompatible Zwecke bestehen. Der Verwalter der Referenzdatenbank ist dafür zuständig, festzulegen, wann und unter welchen Voraussetzungen und für wie lange Gesichtsbilder gespeichert werden dürfen (wobei die Datenaufbewahrungsanforderungen nach zeitlichen oder anderen Kriterien festgelegt werden können).

Da Einsatz und Verwendung von Gesichtserkennungstechnologie hohe inhärente Risiken für die Rechte und Freiheiten der betroffenen Personen innewohnen, sollte die Aufsichtsbehörden für den Datenschutz im Rahmen der vorherigen Konsultation gemäß Art. 28 der JI-Datenschutzrichtlinie einbezogen werden.

2. PROJEKTBEGINN / VOR BESCHAFFUNG DES GESICHTSERKENNUNGSSYSTEMS

Der Prozesseigner in der Strafverfolgungsbehörde sollte sich zuerst ein klares Verständnis des Prozesses bzw. der Prozesse, für die der Einsatz von Gesichtserkennungstechnologie angestrebt wird, verschaffen und sicherstellen, dass es eine Rechtsgrundlage gibt, auf die der beabsichtigte Anwendungsfall gestützt werden kann. Auf dieser Grundlage muss der Prozesseigner dann:

- den Anwendungsfall förmlich beschreiben: Beschreibung des zu lösenden Problems, der Art und Weise, wie die Gesichtserkennungstechnologie die Problemlösung ermöglicht, sowie Überblick über den Prozess (die Aufgabe), in der die Technologie zur Anwendung kommen wird. Dabei sollten die Strafverfolgungsbehörden zumindest Folgendes[73] dokumentieren:
  - die im Prozess aufgezeichneten Kategorien personenbezogener Daten;
  - die Ziele und konkreten Zwecke des Einsatzes von Gesichtserkennungstechnologie, einschließlich der sich nach einem Treffen ergebenden potenziellen Folgen für die betroffene Person;
  - wann und auf welche Weise Gesichtsbilder erfasst werden (einschließlich Angaben zum Erfassungskontext, z. B. am Flugsteig, Tatortvideos aus Sicherheitskameras außerhalb eines Ladengeschäfts usw. sowie die Kategorien betroffener Personen, deren biometrische Daten verarbeitet werden);
  - Die Datenbank für den Bildabgleich (Referenzdatenbank) sowie Angaben zu ihrem Aufbau, ihrer Größe und der Qualität der darin enthaltenen biometrischen Daten;
  - die Akteure in der Strafverfolgungsbehörde, die befugt sind, das Gesichtserkennungssystem zu nutzen und im Rahmen der Strafverfolgung auf dessen Ergebnisse hin zu handeln (die Profile und Zugangsrechte dieser Personen sind vom Prozesseigner festzulegen);
  - die vorgesehene Speicherfrist für die Input-Daten oder das Ereignis, bei dessen Eintritt diese Frist endet (etwa, wenn das Strafverfahren, für das die Daten ursprünglich erhoben wurde, nach dem nationalen Strafprozessrecht abgeschlossen oder eingestellt wird) sowie alle

[73] Anhang I enthält eine Liste von Punkten, die dem Verantwortlichen die Beschreibung von Anwendungsfällen für Gesichtserkennungstechnologie erleichtert.

Folgemaßnahmen (Löschung der Daten, Anonymisierung und Verwendung zu Forschungszwecken oder statistischen Zwecken usw.);
    - die Implementierung der Protokollierung und Zugriff auf Protokolle und Aufzeichnungen;
    - die Performance-Metriken (z. B. Accuracy, Precision, Recall, F1) und ab welchen Mindestwerten diese jeweils akzeptabel sind.[74]
    - Eine Schätzung der Zahl der Personen, die in einem bestimmten Zeitraum / bei einem bestimmten Ereignis von der Gesichtserkennungstechnologie erfasst werden.
- Prüfung der Erforderlichkeit und Verhältnismäßigkeit[75]: Die Technologie sollte nicht vor allem deshalb eingesetzt werden, weil es sie gibt. Der Prozesseigner muss zunächst beurteilen, ob es eine geeignete Rechtsgrundlage für die vorgesehene Verarbeitung gibt. Dazu sind der Datenschutzbeauftragte und die Rechtsabteilung zu konsultieren. Der Antrieb für die Anwendung von Gesichtserkennungstechnologie sollte sein, dass sie eine erforderliche und verhältnismäßige Lösung für ein von der Strafverfolgungsbehörde definiertes spezifisches Problem bietet. Für diese Beurteilung ist auf den Zweck / die Schwere der Straftat / die Anzahl der Personen, die nicht an der Straftat beteiligt, aber dennoch vom Gesichtserkennungssystem betroffen sind, abzustellen. Bei der Rechtmäßigkeitsprüfung ist zumindest Folgendes zu berücksichtigen: JI-Datenschutzrichtlinie[76], DSGVO[77] [78] alle bestehenden rechtlichen Vorschriften zu KI[79] sowie alle von Aufsichtsbehörden für den Datenschutz herausgegebenen einschlägigen Leitlinien (wie etwa die vom EDSA herausgegebenen Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte[80]). Diese Unionsrechtsakte sollten stets in Verbindung mit den einschlägigen nationalen Anforderungen (insbesondere im Bereich des Strafprozessrechts) angewandt werden. Bei der Verhältnismäßigkeitsprüfung ist anzugeben, welche Grundrechte betroffener Personen (über die Rechte auf Schutz der Privatsphäre und Datenschutz hinaus) berührt sein könnten. Außerdem sollten ggf. die für den Anwendungsfall des Gesichtserkennungssystems geltenden

[74] Es gibt verschiedene Metriken für die Evaluierung der Leistungsfähigkeit von Gesichtserkennungssystemen. Jede Metrik betrachtet die Systemergebnisse aus einem anderen Blickwinkel. Inwieweit die Metrik geeignet ist, angemessenen Aufschluss darüber zu geben, ob das Gesichtserkennungssystem gut funktioniert oder nicht, hängt vom jeweiligen Anwendungsfall der Gesichtserkennungstechnologie ab. Liegt der Fokus darauf, eine hohe Trefferquote bei der richtigen Gesichtszuordnung zu erzielen, könnte man die Metriken Precision und Recall verwenden. Diese Metriken erfassen allerdings nicht die Leistung der Gesichtserkennungstechnologie in Bezug auf Falschtreffer (d. h. wie viele Gesichter vom System falsch zugeordnet wurden). Der Prozesseigner dürfte mit Unterstützung durch die Abteilung für IT, KI und/oder Datenwissenschaft in der Lage sein, die Leistungsanforderungen festzulegen und diese in der Metrik auszudrücken, die für den betreffenden Anwendungsfall der Gesichtserkennungstechnologie am besten geeignet ist.

[75] In Betracht kommen auch weitere Maßnahmen im Hinblick auf die Erforderlichkeit, etwa was Zuschnitt und Verwendung des Systems angeht; die Beschreibung des Anwendungsfalls kann sich also im Zuge der Erforderlichkeits- und Verhältnismäßigkeitsprüfung auch noch leicht ändern.

[76] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.

[77] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[78] In Fällen, in denen für ein wissenschaftliches Projekt zur Erforschung der Verwendung von Gesichtserkennungstechnologie personenbezogene Daten verarbeitet werden müssten, diese Verarbeitung jedoch nicht allgemein unter Artikel 4 Absatz 3 der JI-Datenschutzrichtlinie fiele, wäre die DSGVO anwendbar (Artikel 9 Absatz 2 der JI-Datenschutzrichtlinie). Im Falle von Pilotprojekten, an die sich Strafverfolgungsmaßnahmen anschlössen, wäre die JI-Datenschutzrichtlinie weiterhin anwendbar.

[79] Zum Beispiel gibt es einen Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION, der allerdings noch nicht als Verordnung angenommen wurde.

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

Einschränkungen beschrieben und diese Einschränkungen (oder das Fehlen solcher Einschränkungen) berücksichtigt werden (z. B., ob das System dauerhaft oder vorübergehend betrieben werden wird und ob es auf einen bestimmten räumlichen Bereich beschränkt sein wird).

- Durchführung einer Datenschutz-Folgenabschätzung (DSFA) [81]: Es ist eine DSFA durchzuführen, weil der Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung mit hoher Wahrscheinlichkeit ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen birgt[82]. Die DSFA sollte insbesondere Folgendes enthalten: eine allgemeine Beschreibung der vorgesehenen Verarbeitungsvorgänge[83], eine Beurteilung der Risiken für die Rechte und Freiheiten betroffener Personen[84], die vorgesehenen Risikominderungsmaßnahmen, Garantien und Sicherheitsmaßnahmen sowie Mechanismen zur Gewährleistung des Schutzes personenbezogener Daten und zum Nachweis der Vorschriftseinhaltung. Die DSFA ist ein laufender Prozess, dem ggf. neue Verarbeitungselemente hinzuzufügen sind, wobei die Risikobewertung in jeder Projektphase zu aktualisieren ist.
- Genehmigungseinholung bei der obersten Leitung, wobei die Risiken, die sich (aus dem Anwendungsfall und der Technologie) für die Rechte und Freiheiten betroffener Personen ergeben, sowie die jeweiligen Risikominderungspläne zu erklären sind.

3. WÄHREND DER BESCHAFFUNG UND VOR EINSATZ DER GESICHTSERKENNUNGSTECHNOLOGIE

- Entscheidung über die Kriterien für die Auswahl der Gesichtserkennungstechnologie (Algorithmus): Die Entscheidung über die Kriterien für die Algorithmusauswahl sollte vom Prozesseigner getroffen werden, mit Unterstützung durch die Abteilung für IT, KI und/oder Datenwissenschaft. In der Praxis würden diese Kriterien die in der Beschreibung des Anwendungsfalls festgelegten Metriken für Fairness und Leistungsfähigkeit umfassen. Die Kriterien sollten auch Angaben zu den Daten enthalten, mit denen der Algorithmus trainiert wurde. Der Datensatz für Training, Tests und Validierung muss hinreichend Samples für alle Merkmale der betroffenen Personen enthalten, auf die die Gesichtserkennungstechnologie angewendet werden soll (z. B. im Hinblick auf Alter, Geschlecht, Rasse), um Verzerrungen (Bias) zu reduzieren. Der Anbieter der Gesichtserkennungstechnologie sollte Angaben und Metriken zu den Datensätzen für Training, Tests und Validierung liefern und beschreiben, welche Maßnahmen

[81] Weitere Leitlinien zu DSFA sind zu finden unter: Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 rev.01, abrufbar unter: https://ec.europa.eu/newsroom/article29/items/611236, sowie EDSB, Rechenschaftspflicht in der Praxis Teil II: Datenschutz-Folgenabschätzung und vorherige Konsultation, abrufbar unter: https://edps.europa.eu/node/4582_en.

[82] Bei Gesichtserkennungstechnologie können je nach Anwendungsfall folgende Kriterien erfüllt sein, bei denen die Verarbeitung ein hohes Risiko mit sich bringt (entnommen aus den Leitlinien zur DSFA, WP 248 rev.01): systematische Überwachung, Datenverarbeitung in großem Umfang, Abgleichen oder Zusammenführen von Datensätzen, innovative Nutzung oder Anwendung technologischer oder organisatorischer Lösungen.

[83] Abgesehen von der Risikobewertung sind auch die Beschreibung der Verarbeitung sowie die bereits in den vorstehenden Schritten beschriebene Erforderlichkeits- und Verhältnismäßigkeitsprüfung Teil der DSFA. Erforderlichenfalls enthält die DSFA eine detailliertere Beschreibung der Ströme personenbezogener Daten.

[84] Die Analyse der Risiken für betroffene Personen sollte auch die Risiken berücksichtigen, die sich aus dem Ort (lokal / aus der Ferne) ergeben, an dem die Gesichtsbilder abgeglichen werden, wie auch die Risiken in Bezug auf Auftragsverarbeiter/Unterauftragsverarbeiter sowie, soweit maschinelles Lernen zur Anwendung kommt, dessen spezifische Risiken (z. B. Data Poisoning (Datenvergiftung), Adversarial Examples (kontradiktorische Beispiele)).

ergriffen wurden, um potenzielle rechtswidrige Diskriminierung und Bias zu messen und zu mindern. Der Prozesseigner muss nach Möglichkeit (auf Grundlage der vom Anbieter zur Verfügung gestellten Informationen) prüfen, ob der Anbieter seine Verwendung dieses Datensatzes für das Trainieren der Algorithmen auf eine Rechtsgrundlage stützen konnte. Der Prozesseigner sollte auch sicherstellen, dass der Anbieter der Gesichtserkennungstechnologie für biometrische Daten geltende Sicherheitsstandards wie ISO/IEC 24745 anwendet, die sowohl Leitlinien dafür enthalten, wie biometrische Informationen bei der Speicherung und Übermittlung im Hinblick auf unterschiedliche Anforderungen an Vertraulichkeit, Integrität und Wiederherstellbarkeit/Widerruflichkeit zu schützen sind, als auch Leitlinien für sichere und privatsphärengerechte Verwaltung und Verarbeitung biometrischer Informationen.

- Algorithmus neu trainieren (sofern erforderlich): Der Prozesseigner sollte auch darauf achten, dass der Lieferumfang das Feintuning des Gesichtserkennungssystems einschließt, das vor dessen Einsatz erfolgt, um eine höhere Accuracy zu erzielen. Ist zusätzliches Training nötig, damit das erworbene Gesichtserkennungssystem die Accuracy-Metriken erreicht, so muss der Prozesseigner (abgesehen von der Entscheidung für neuerliches Training) auch – mithilfe der Abteilung für IT, KI und/oder Datenwissenschaft – eine Entscheidung über den dafür zu verwendenden angemessenen repräsentativen Datensatz treffen und prüfen, ob eine derartige Verwendung der Daten rechtmäßig ist.
- Festlegung geeigneter Garantien zur Minderung von Risiken in Bezug auf Sicherheit, Bias und geringe Leistungsfähigkeit Hierzu gehört die Aufstellung eines Verfahrens, nach dem die Gesichtserkennungstechnologie im Einsatz überwacht wird (Protokollierung und Feedback hinsichtlich der Accuracy und Fairness der Ergebnisse). Darüber hinaus ist sicherzustellen, dass die spezifisch mit maschinellem Lernen und Gesichtserkennungssystemen verbundenen Risiken (z. B. Data Poisoning (Datenvergiftung), Adversarial Examples (kontradiktorische Beispiele), Model Inversion (Rekonstruktion von Trainingsdaten), White-Box Inference) erkannt, gemessen und gemindert werden. Der Prozesseigner sollte auch geeignete Garantien vorsehen, um sicherzustellen, dass die Anforderungen, die für die Speicherung der biometrischen Daten im Datensatz für das erneute Training gelten, eingehalten werden.
- Dokumentation des Gesichtserkennungssystems: Diese sollte eine allgemeine Beschreibung des Gesichtserkennungssystems, eine detaillierte Beschreibung der Elemente des Gesichtserkennungssystems und des Verfahrens für seinen Aufbau, detaillierte Angaben zu Überwachung, Funktionsweise und Kontrolle über das Gesichtserkennungssystem sowie eine detaillierte Beschreibung seiner Risiken und der Risikominderungsmaßnahmen enthalten. Die in dieser Dokumentation enthaltenen Elemente umfassen die Hauptelemente der Beschreibung des Gesichtserkennungssystems aus den vorhergehenden Phasen (siehe oben), die jedoch um Informationen bezüglich der Überwachungsleistung und der Vornahme von Systemänderungen (u. a. Versions-Updates und/oder neues Training) zu ergänzen sind.
- Erstellung von Nutzerhandbüchern, Erklärung der Technologie und der Anwendungsfälle: Hier sind sämtliche Szenarien für die Verwendung von Gesichtserkennungstechnologie und die dafür geltenden Voraussetzungen in gut verständlicher Weise zu erklären.
- Schulung der Endnutzer über die Anwendung der Technologie: In diesen Schulungen sind die Möglichkeiten und Grenzen der Technologie zu erklären, damit die Nutzer verstehen, unter welchen Umständen deren Anwendung erforderlich ist und in welchen Fällen es vorkommen kann, dass die Technologie unrichtige Ergebnisse liefert. Derartige Schulungen tragen auch dazu bei, den Risiken entgegenzuwirken, die sich ergeben, wenn Algorithmusergebnisse nicht überprüft/kritisch hinterfragt werden.
- Vorherige Konsultation der Aufsichtsbehörde für den Datenschutz gemäß Artikel 28 Absatz 1 Buchstabe b der JI-Datenschutzrichtlinie. Information gemäß Artikel 13 der JI-Datenschutzrichtlinie, um die betroffenen Personen über die Verarbeitung und ihre Rechte zu informieren. In diesen Hinweisen sind die betroffenen Personen in angemessener und

verständlicher Sprache über die Verarbeitung aufzuklären, unter Erläuterung der Grundelemente der Technologie (u. a. Trefferquoten und Trainingsdatensätze sowie die zur Vermeidung von Diskriminierung und geringer Accuracy des Algorithmus ergriffenen Maßnahmen).

4. EMPFEHLUNGEN NACH EINSATZ DER GESICHTSERKENNUNGSTECHNOLOGIE

- Persönliches Eingreifen und Ergebnisüberprüfung: Gegen eine Person dürfen niemals Maßnahmen ergriffen werden, die ausschließlich auf dem Ergebnis der Gesichtserkennungstechnologie beruhen (andernfalls hätte eine automatisierte Entscheidungsfindung im Einzelfall rechtliche oder vergleichbare Auswirkungen auf die betroffene Person, was gegen Artikel 11 der JI-Datenschutzrichtlinie verstieße). Es ist sicherzustellen, dass die Ergebnisse der Gesichtserkennungstechnologie von einem Beamten der Strafverfolgungsbehörde überprüft werden. Des Weiteren ist sicherzustellen, dass diejenigen in der Strafverfolgungsbehörde, die die Technologie nutzen, nicht der Maschinengläubigkeit verfallen, sondern widersprüchlichen Informationen nachgehen und die Ergebnisse der Technologie kritisch überprüfen. Dies erfordert nicht nur ständige Schulungen und Aufklärung der Endnutzer, sondern auch die Bereitstellung angemessener, zur wirksamen Überprüfung fähiger personeller Ressourcen durch die oberste Leitung. Das erfordert, dass jeder Beamte genügend Zeit haben muss, die von der Technologie gelieferten Ergebnisse kritisch zu hinterfragen. Es ist zu erfassen, zu messen und zu bewerten, in welchem Umfang die ursprüngliche mit Gesichtserkennungstechnologie getroffene Entscheidung nach menschlicher Überprüfung abgeändert wurde.
- Überwachung Maßnahmen gegen Model Drift (Leistungsverschlechterung) nach Inbetriebnahme des Modells.
- Aufstellung eines Verfahrens für die Neubewertung der Risiken und der Sicherheitsmaßnahmen, sowohl in regelmäßigen Abständen als auch bei jeder Veränderung der Technologie oder des Anwendungsfalls.
- Dokumentierung jeder Systemänderung während des gesamten Lebenszyklus (z. B. Upgrades, Re-Training).
- Aufstellung eines Verfahrens sowie der dazugehörigen technischen Fähigkeiten zur Beantwortung von Auskunftsverlangen betroffener Personen. Die technische Fähigkeit zur Datenextraktion, um erforderlichenfalls betroffenen Personen Daten zur Verfügung stellen können, muss gegeben sein, bevor ein Auskunftsverlangen eingeht.
- Es ist sicherzustellen, dass für den Fall von Datenschutzverletzungen einschlägige Verfahren vorgesehen sind. Sollte der Schutz personenbezogener Daten (einschließlich biometrischer Daten) verletzt werden, sind die Risiken wahrscheinlich hoch. In einem solchen Fall sollten alle Nutzer die einschlägigen Verfahren kennen, die dann zu befolgen sind; der Datenschutzbeauftragte ist sofort zu verständigen und auch die betroffenen Personen sind zu benachrichtigen.

ANHANG III – PRAKTISCHE BEISPIELE

In der Praxis gibt es viele verschiedene Situationen und Zwecke für den Einsatz von Gesichtserkennung, zum Beispiel in kontrollierten Umgebungen wie Grenzübergangsstellen, beim Datenabgleich mit Daten aus anderen Polizeidatenbanken oder wenn personenbezogene Daten von der betroffenen Person offensichtlich öffentlich gemacht wurden, bei Übertragung von Kamerabildern in Echtzeit (Gesichtserkennung in Echtzeit) usw. Deshalb sind die Risiken für den Schutz personenbezogener Daten und anderer Grundrechte und Freiheiten je nach den verschiedenen Anwendungsfällen sehr verschieden. Zur Erleichterung der Erforderlichkeits- und Verhältnismäßigkeitsprüfung, die jeweils vor der Entscheidung über den möglichen Einsatz von Gesichtserkennung durchzuführen ist, enthalten diese Leitlinien eine nicht erschöpfende Auflistung möglicher Anwendungen von Gesichtserkennungstechnologie im Bereich der Strafverfolgung.

Die Szenarien, die hier vorgestellt und bewertet werden, beruhen auf **hypothetischen** Situationen. Sie sollen konkrete Anwendungen von Gesichtserkennungstechnologie anschaulich darstellen und nicht nur bei der Abwägung im Einzelfall helfen, sondern auch einen allgemeinen Rahmen setzen. Es ist nicht angestrebt, einen erschöpfenden Überblick zu geben. Diese Beispiele stehen auch unter dem Vorbehalt laufender oder künftiger Verfahren, die nationale Aufsichtsbehörden im Hinblick auf die Gestaltung, Erprobung oder Implementierung von Gesichtserkennungstechnologie durchführen mögen. Die hier vorgestellten Szenarien sollen lediglich dazu dienen, den Politikern, Gesetzgebern und Strafverfolgungsbehörden anschauliche Beispiele für die in diesem Dokument aufgestellten Leitlinien zu geben, um sicherzustellen, dass diese die unionsrechtlichen Vorschriften über den Schutz personenbezogener Daten vollständig einhalten, wenn sie Gesichtserkennungstechnologie gestalten und deren Implementierung vorsehen. In diesem Zusammenhang ist zu bedenken, dass, selbst wenn Gesichtserkennungstechnologie in recht ähnlichen Situationen eingesetzt wird, das Vorhandensein (oder Fehlen) gewisser Umstände dazu führen kann, dass das Ergebnis der Erforderlichkeits- und Verhältnismäßigkeitsprüfung ganz anders ausfällt.

1 SZENARIO 1

1.1. Beschreibung

Ein automatisches Grenzkontrollsystem, das den Grenzübertritt nach automatischer Kontrolle ermöglicht, indem das biometrische Bild, das im elektronischen Reisedokument von Unionsbürgern und anderen die Grenze übertretenden Reisenden gespeichert ist, authentifiziert wird, um festzustellen, dass der Grenzgänger der rechtmäßige Inhaber des Dokuments ist.

Bei einer solchen Verifizierung/Authentifikation handelt es sich um eine One-to-One-Gesichtserkennung, die in kontrollierter Umgebung (z. B. an e-Gates in Flughäfen) erfolgt. Die biometrischen Daten der Reisenden, die die Grenze übertreten, werden jeweils erfasst, indem diese ausdrücklich aufgefordert werden, in die Kamera im e-Gate zu blicken; die Daten werden dann mit denen im vorgelegten Dokument (Reisepass, Personalausweis usw.) abgeglichen, das jeweils nach bestimmten technischen Vorgaben ausgestellt wird.

Während die Verarbeitung in solchen Fällen grundsätzlich außerhalb des Anwendungsbereichs der JI-Datenschutzrichtlinie liegt, kann das Ergebnis der Verifizierung im Rahmen des Grenzschutzes auch dazu verwendet werden, (alphanumerische) Daten der Person mit Strafverfolgungsdatenbanken abzugleichen, sodass es also zu Maßnahmen kommen kann, die erhebliche rechtliche Auswirkungen auf die betroffene Person haben, zum Beispiel zur Festnahme wegen einer SIS-II-Ausschreibung. Unter

bestimmten Umständen können biometrische Daten auch für Abgleiche mit anderen Strafverfolgungsdatenbanken verwendet werden (in solchen Fällen würde in diesem Schritt eine One-to-Many-Identifikation erfolgen).

Das Ergebnis der Verarbeitung biometrischer Bilder hat unmittelbare Auswirkungen auf die betroffene Person, da diese die Grenze nur passieren darf, wenn die Verifizierung gelingt. Scheitert die Identifikation, müssen die Grenzbeamten eine zweite Überprüfung vornehmen, um sich zu vergewissern, dass die betroffene Person tatsächlich nicht dieselbe ist, die auf dem Ausweisdokument abgebildet ist.

Wird ein Treffer für eine SIS-II-Ausschreibung oder nationale Ausschreibung angezeigt, so müssen die Grenzbeamten eine zweite Verifizierung und die erforderlichen weiteren Überprüfungen vornehmen und dann alle erforderlichen Maßnahmen ergreifen, zum Beispiel die Person festnehmen und die betroffenen Behörden verständigen.

Informationsquelle:
- Arten betroffener Personen: ☒ alle Grenzgänger an der Grenzübergangsstelle
- Bildquelle: ☒ sonstige (Identitätsausweis)
- Bezug zur Straftat: ☒ nicht erforderlich
- Art der Informationserfassung: ☒ in einer Kabine oder in kontrollierter Umgebung
- Kontext – Eingriff in andere Grundrechte: Ja, nämlich: ☒ Recht auf Freizügigkeit ☒ Asylrecht

Referenzdatenbank (für den Abgleich der erfassten Informationen):
- Spezifizität: ☒ spezifische Grenzschutzdatenbanken

Algorithmus:
- Art der Verifizierung: ☒ One-to-One-Verifizierung (Authentifikation)

Ergebnis:
- Auswirkung ☒ unmittelbar (die Einreise wird der betroffenen Person gestattet oder verweigert)
- Automatisierte Entscheidung: ☒ Ja

1.2. Einschlägiger rechtlicher Rahmen

Seit 2004 müssen gemäß Verordnung (EG) Nr. 2252/2004 des Rates[85] von den Mitgliedstaaten ausgegebene Pässe und Reisedokumente ein biometrisches Gesichtsbild enthalten, das in einem elektronischen Chip gespeichert ist, der in das Dokument eingebettet ist.

Im Schengener Grenzkodex (SGK)[86] sind die Anforderungen an Grenzübertrittskontrollen von Personen an den Außengrenzen niedergelegt. Im Falle von Unionsbürgern und anderen Personen, die nach Unionsrecht Anspruch auf freien Personenverkehr haben, sollten die Mindestkontrollen zumindest die Überprüfung ihrer Reisedokumente umfassen, und zwar, soweit angemessen, unter Einsatz technischer Geräte. Der SGK wurde später durch die Verordnung (EU) 2017/2225[87] geändert, mit der unter anderem Begriffsbestimmungen für „e-Gates“, „automatisches Grenzkontrollsystem“ und „Self-

[85] VERORDNUNG (EG) NR. 2252/2004 DES RATES vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten.
[86] VERORDNUNG (EU) 2016/399 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 9. März 2016 über einen Unionskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex).
[87] Verordnung (EU) 2017/2225 des Europäischen Parlaments und des Rates vom 30. November 2017 zur Änderung der Verordnung (EU) 2016/399 in Bezug auf die Nutzung des Einreise-/Ausreisesystems.

Service-System“ sowie die Möglichkeit der Verarbeitung biometrischer Daten für die Durchführung der Grenzübertrittskontrollen eingeführt wurden.

Es konnte also angenommen werden, dass es eine klare und vorhersehbare Rechtsgrundlage gibt, die diese Form der Verarbeitung personenbezogener Daten gestattet. Überdies handelt es sich um einen auf Unionsebene erlassenen Rechtsrahmen, der in den Mitgliedstaaten unmittelbar anwendbar ist.

1.3. Erforderlichkeit und Verhältnismäßigkeit – Zweck/Schwere der Straftat

Die Überprüfung der Identität von Unionsbürgern in einer automatischen Grenzübertrittskontrolle, unter Verwendung ihres biometrischen Bilds, ist ein Element der Grenzübertrittskontrollen an den Außengrenzen der EU. Daraus folgt, dass sie in unmittelbarem Zusammenhang mit der Grenzsicherheit steht und einer von der Union anerkannten, dem Gemeinwohl dienenden Zielsetzung dient. Automatisierte biometriegestützte Grenzkontrollspuren tragen außerdem dazu bei, die Passagierkontrolle zu beschleunigen und die Gefahr menschlicher Fehler zu mindern. Zudem halten sich Bereich, Umfang und Intensität des Eingriffs in diesem Szenario in sehr viel engeren Grenzen als bei anderen Formen der Gesichtserkennung. Dennoch entstehen durch die Verarbeitung biometrischer Daten zusätzliche Risiken für betroffene Personen, die von der zuständigen Behörde, die die Gesichtserkennungstechnologie einsetzt und betreibt, ordnungsgemäß festzustellen und zu mindern sind.

1.4. Ergebnis

Die im Rahmen einer automatisierten Grenzübergangskontrolle durchgeführte Identitätsüberprüfung bei Unionsbürgern ist eine erforderliche und verhältnismäßige Maßnahme, solange es geeignete Garantien gibt, und zwar insbesondere durch Anwendung der Zweckbindungs-, Datenqualitäts- und Transparenzgrundsätze sowie ein hohes Sicherheitsniveau.

2 SZENARIO 2

2.1. Beschreibung

Strafverfolgungsbehörden richten ein System zur Identifikation der Opfer von Kindesentführungen ein. Unter strengen Voraussetzungen können befugte Polizeibeamte die biometrischen Daten eines mutmaßlich entführten Kindes mit einer Datenbank für Opfer von Kindesentführungen abgleichen, und zwar ausschließlich zu dem Zweck, Minderjährige zu identifizieren, auf die die Beschreibung eines vermissten Kindes zutrifft, in dessen Fall ein Ermittlungsverfahren eingeleitet und die Fahndung ausgeschrieben wurde.

Die in Rede stehende Verarbeitung wäre der Abgleich des Gesichts oder Bildes einer natürlichen Person, auf die möglicherweise die Beschreibung eines vermissten Kindes zutrifft, mit in einer Datenbank gespeicherten Bildern. Eine solche Verarbeitung würde nur in bestimmten Fällen – und nicht systematisch – erfolgen.

Die Datenbank, mit der der Abgleich vorgenommen wird, ist mit Bildern vermisster Kinder populiert, für die ein Verdacht auf Kindesentführung bzw. eine Gefahr für Leib oder Leben gemeldet und eine einer Justizbehörde unterliegende strafrechtliche Ermittlung eingeleitet wurde und die wegen Kindesentführung zur Fahndung ausgeschrieben wurden. Die Daten werden im Rahmen der Verfahren der zuständigen Strafverfolgungsbehörden erhoben, d. h. durch zur Wahrnehmung polizeilicher Aufgaben befugte Polizeibeamte. Aufgezeichnet werden folgende Kategorien personenbezogener Daten:

- Identität, Spitzname, Aliasname, Abstammung, Staatsangehörigkeit, Anschriften, E-Mail-Adressen, Telefonnummern;
- Geburtsdatum und Geburtsort;
- Angaben zu den Eltern;
- Foto mit technischen Merkmalen für die Verwendung eines Gesichtserkennungsgeräts sowie andere Fotos.

Die Abgleichergebnisse müssen auch von einem befugten Beamten überprüft und verifiziert werden, um frühere Beweise mittels des Abgleichergebnisses zu bestätigen und etwaige Falschtreffer auszuschließen.

Die Bilder und personenbezogenen Daten der Kinder dürfen nur für die Dauer der Fahndung gespeichert werden; wird das Strafverfahren, in dessen Zuge die Bilder in die Datenbank aufgenommen wurde, nach den nationalen Vorschriften abgeschlossen oder eingestellt, müssen die Bilder sofort gelöscht werden.

Auch wenn für die biometrischen Daten in der Datenbank im nationalen Recht eine vergleichsweise lange Speicherfrist vorgesehen sein mag, bieten die Ausübung der Rechte betroffener Personen und insbesondere das Recht auf Berichtung und Löschung eine zusätzliche Garantie, die dem Eingriff in das Recht auf den Schutz der personenbezogenen Daten der betroffenen Personen Schranken setzt.

Informationsquelle:
- Arten betroffener Personen: ☒ Kinder
- Bildquelle ☒ sonstige: nicht vorab definiert, mutmaßliches Opfer einer Kindesentführung
- Bezug zur Straftat ☒ kein unmittelbarer zeitlicher Bezug ☒ kein unmittelbarer räumlicher Bezug
- Art der Informationserfassung: ☒ in einer Kabine oder in kontrollierter Umgebung
- Kontext: Eingriff in andere Grundrechte: ☒ Ja, nämlich: ☒ verschiedene

Referenzdatenbank (für den Abgleich der erfassten Informationen):
- Spezifizität ☒ spezifische Datenbank

Algorithmus:
- Art der Verifizierung: ☒ One-to-Many-Identifikation

Ergebnis:
- Auswirkungen ☒ unmittelbar
- Automatisierte Entscheidung: ☒ NEIN, zwingende Überprüfung durch befugten Beamten

Rechtliche Prüfung:
- Einschlägiger rechtlicher Rahmen: ☒ Besondere nationale Rechtsvorschriften für diese Verarbeitung (Gesichtserkennung)

2.2. Einschlägiger rechtlicher Rahmen

Das nationale Recht sieht einen speziellen rechtlichen Rahmen vor, in dem die Einrichtung der Datenbank geregelt und sowohl die Verarbeitungszwecke als auch die Kriterien für die Populierung der Datenbank, den Zugang zur Datenbank und deren Verwendung festgelegt sind. Die für deren Implementierung erforderlichen Gesetzgebungsmaßnahmen sehen auch Regelungen für die Festlegung der Speicherfrist vor und nehmen Bezug auf die einschlägigen Grundsätze der Integrität

und Vertraulichkeit. Außerdem sind in den Gesetzgebungsmaßnahmen die Modalitäten für die Unterrichtung der betroffenen Personen und, in diesem Fall, der Inhaber der elterlichen Sorge sowie die Ausübung der Rechte betroffener Personen und ggf. etwaige Beschränkungen vorgesehen. Im Zuge der Ausarbeitung des Vorschlags für die betreffende Gesetzgebungsmaßnahme musste die nationale Aufsichtsbehörde konsultiert werden.

2.3. Erforderlichkeit und Verhältnismäßigkeit – Zweck/Schwere der Straftat / Zahl der von der Verarbeitung betroffenen Personen, die nicht an Straftaten beteiligt sind

Verarbeitungsvoraussetzungen und Garantien

Der auf Gesichtserkennung beruhende Abgleich darf nur von einem befugten Beamten und auch nur als letztes Mittel vorgenommen werden, wenn keine weniger eingreifenden Mittel zur Verfügung stehen und der Abgleich unbedingt erforderlich ist, wenn zum Beispiel Zweifel an der Echtheit des Identitätsdokuments des reisenden Minderjährigen bestehen und/oder wenn die Prüfung bereits gesammelter Beweise und Materialien ergeben hat, dass möglicherweise eine Übereinstimmung mit der Beschreibung eines vermissten Kindes besteht, dessentwegen strafrechtliche Ermittlungen laufen.

Eine zusätzliche Garantie ergibt sich aus der Vorschrift, dass der mittels Gesichtserkennung durchgeführte Abgleich zwingend von einem befugten Beamten überprüft und verifiziert werden muss, um frühere Beweise mittels des Abgleichergebnisses zu bestätigen und etwaige Falschtreffer auszuschließen.

Verfolgtes Ziel

Die Einrichtung der Datenbank dient wichtigen Zielen des allgemeinen öffentlichen Interesses, insbesondere der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie dem Schutz der Rechte und Freiheiten anderer. Die Einrichtung der Datenbank und die vorgesehene Verarbeitung tragen ersichtlich zur Identifikation von Kindern, die Entführungsopfer sind, bei und können deshalb als Maßnahme angesehen werden, die geeignet ist, das legitime Ziel der Ermittlung und Verfolgung solcher Straftaten zu fördern.

Zweck und Populierung der Datenbank

Die Verarbeitungszwecke sind eindeutig gesetzlich festgelegt; die Datenbank darf ausschließlich zu dem Zweck verwendet werden, Kinder zu identifizieren, die als mutmaßliche Opfer von Kindesentführung als vermisst gemeldet sind und derentwegen eine der Aufsicht einer Justizbehörde unterliegende strafrechtliche Ermittlung eingeleitet wurde und die wegen Kindesentführung zur Fahndung ausgeschrieben sind. Die im Gesetz vorgesehenen Voraussetzungen für die Populierung der Datenbank zielen darauf ab, die Zahl der betroffenen Personen und personenbezogenen Daten, die in die Datenbank aufgenommen werden, strikt zu begrenzen. Der Inhaber der elterlichen Sorge für das Kind ist über die vorgenommene Verarbeitung zu unterrichten sowie über die Voraussetzungen für die Ausübung der Rechte des Kindes in Bezug auf die für Identifikationszwecke vorgesehene Verarbeitung biometrischer Daten oder auf die in der Datenbank gespeicherten personenbezogenen Daten des Kindes.

2.4. Ergebnis

Im Hinblick auf die Erforderlichkeit und Verhältnismäßigkeit der vorgesehenen Verarbeitung sowie das Kindeswohl in Bezug auf diese Verarbeitung personenbezogener Daten und unter der Voraussetzung, dass es hinreichend Garantien gibt, die die Ausübung der Rechte betroffener Personen sicherstellen

(insbesondere unter Berücksichtigung des Umstands, dass es um die Verarbeitung der Daten von Kindern geht), kann eine solche Anwendung der Verarbeitung von Gesichtserkennungsdaten als wahrscheinlich mit dem Unionsrecht vereinbar angesehen werden.

Angesichts der Art der Verarbeitung und der eingesetzten Technologie, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, ist der EDSA des Weiteren der Ansicht, dass die Ausarbeitung des Vorschlags für eine vom nationalen Parlament zu beschließende Gesetzgebungsmaßnahme oder für eine auf einer solchen Gesetzgebungsmaßnahme beruhende Regelungsmaßnahme, die sich auf die vorgesehene Verarbeitung bezieht, eine vorherige Konsultation der Aufsichtsbehörde umfassen muss, um die Übereinstimmung mit dem einschlägigen rechtlichen Rahmen und dessen Einhaltung sicherzustellen (vgl. Artikel 28 Absatz 2 der JI-Datenschutzrichtlinie).

3 SZENARIO 3

3.1. Beschreibung

Im Zuge polizeilicher Maßnahmen bei gewalttätigen Ausschreitungen und anschließender Ermittlungen wurden mehrere Personen als Verdächtige ermittelt, z. B. auf Grundlage früherer Ermittlungen, bei denen Material aus Videoüberwachungsanlagen oder Zeugenaussagen verwendet wurde. Die Bilder dieser Verdächtigen werden mit den Bildern von Personen abgeglichen, die am Tatort oder in dessen Umgebung von Videoüberwachungsanlagen oder Mobilgeräten aufgenommen wurden.

Die Polizei will genaueres Beweismaterial zu den Personen erlangen, die im Verdacht stehen, an den gewalttätigen Ausschreitungen im Umfeld einer Demonstration teilgenommen zu haben. Sie richtet deshalb eine Datenbank mit Bildmaterial ein, das in lockerem räumlichen und zeitlichen Zusammenhang zu den gewalttätigen Ausschreitungen steht. Die Datenbank enthält private Aufzeichnungen, die von Bürgern auf der Polizei-Website hochgeladen wurden, Material aus im öffentlichen Personenverkehr eingesetzten Videoüberwachungsanlagen, polizeieigenes Videoüberwachungsmaterial sowie von Medien veröffentlichtes Material; es gibt keine spezifischen Einschränkungen oder Garantien. Die Aufnahme von Dateien in die Datenbank setzt nicht voraus, dass darauf die Begehung schwerer Straftaten zu sehen ist. Deshalb sind in der Datenbank auch gar nicht an den gewalttätigen Ausschreitungen beteiligte Personen gespeichert, die einen erheblichen Prozentsatz der örtlichen Bevölkerung ausmachen, die zum Zeitpunkt der Demonstration als Passanten oder als nicht an den gewalttätigen Ausschreitungen beteiligte Demonstranten zugegen waren. Insgesamt handelt es sich um Tausende Video- und Bilddateien.

Mit Gesichtserkennungssoftware werden allen in diesen Dateien zu sehenden Gesichtern eindeutige Gesichts-IDs zugewiesen. Die Gesichter der einzelnen Verdächtigen werden sodann automatisch mit diesen Gesichts-IDs abgeglichen. Die Datenbank, die alle biometrischen Templates in den Tausenden Video- und Bilddateien umfasst, wird gespeichert, bis alle in Betracht kommenden Ermittlungen beendet sind. Treffer werden von den zuständigen Beamten bearbeitet, die dann über das weitere Vorgehen entscheiden. In diesem Zuge kann die in der Datenbank gefundene Datei der Ermittlungsakte der betreffenden Person zugeordnet werden, es kommen aber auch andere Maßnahmen in Betracht, zum Beispiel die Vernehmung oder Festnahme der betreffenden Person.

Es gibt ein nationales Gesetz, das eine allgemeine Bestimmung enthält, nach der die Verarbeitung biometrischer Daten für die Zwecke der eindeutigen Identifikation einer natürlichen Person zulässig ist, sofern diese unbedingt erforderlich ist und es geeignete Garantien für die Rechte und Freiheiten der betroffenen Person gibt.

Informationsquelle:

- Arten betroffener Personen: ☒ alle Personen
- Bildquelle: ☒ frei zugängliche Flächen/Räume ☒ private Einrichtung ☒ andere natürliche Personen ☒ sonstige: Medien
- Bezug zur Straftat: ☒ Nicht notwendigerweise unmittelbarer räumlicher oder zeitlicher Bezug
- Art der Informationserfassung: ☒ aus der Ferne
- Kontext – Eingriff in andere Grundrechte: Ja, nämlich ☒ Kontext: Versammlungsfreiheit
- Etwaige zusätzliche Informationsquellen bezüglich der betroffenen Person: ☒ sonstige: nicht ausgeschlossen (etwa Benutzung von Geldautomaten, aufgesuchte Geschäfte), da keine Kontrolle über das auf den Bildern Abgebildete besteht

Referenzdatenbank (für den Abgleich der erfassten Informationen):

- Spezifizität: ☒ spezifische Datenbanken für den Kriminalitätsbereich

Algorithmus:

- Art der Verarbeitung: ☒ One-to-Many-Identifikation

Ergebnis:

- Auswirkungen: ☒ unmittelbare Auswirkungen (z. B. Festnahme, Vernehmung der betroffenen Personen)
- Automatisierte Entscheidung: ☒ NEIN
- Speicherfrist: bis alle in Betracht kommenden Ermittlungen beendet sind

Rechtliche Prüfung:

- Art der Vorabinformation der betroffenen Person: ☒ Allgemeine Informationen auf der Website der Strafverfolgungsbehörde
- Einschlägiger rechtlicher Rahmen: ☒ JI-Datenschutzrichtlinie weitgehend wortgleich ins nationale Recht übernommen ☒ Allgemeines nationales Gesetz für die Verwendung biometrischer Daten durch Strafverfolgungsbehörden

3.2. Einschlägiger rechtlicher Rahmen

Wie oben bereits aufgezeigt wurde, sind Rechtsgrundlagen, die lediglich die Generalklausel in Artikel 10 der JI-Datenschutzrichtlinie wiederholen, nicht hinreichend deutlich formuliert, den natürlichen Personen hinreichend Aufschluss darüber zu geben, unter welchen Voraussetzungen und Umständen Strafverfolgungsbehörden befugt sind, Aufzeichnungen aus Videoüberwachungsanlagen auf frei zugänglichen Flächen dazu zu verwenden, ein biometrisches Template des Gesichts der Person anzufertigen und dieses mit Polizeidatenbanken, anderen verfügbaren Aufnahmen aus Videoüberwachungsanlagen oder privaten Aufzeichnungen usw. abzugleichen. Der in diesem Szenario gegebene rechtliche Rahmen genügt deshalb nicht den Mindestanforderungen an eine Rechtsgrundlage.

3.3. Erforderlichkeit und Verhältnismäßigkeit

In diesem Beispiel gibt die Verarbeitung aus mehreren Gründen Anlass zu Bedenken im Hinblick auf die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit:

Die Personen sind keiner schweren Straftat verdächtig. Die Aufnahme von Dateien in die Datenbank mit dem Bildmaterial setzt nicht voraus, dass auf dem Bildmaterial die Begehung schwerer Straftaten

zu sehen ist. Die Verwendung der Dateien in der Datenbank ist auch nicht an die Voraussetzung geknüpft, dass diese in unmittelbarem zeitlichem oder räumlichem Zusammenhang mit der Straftat stehen. Dies führt dazu, dass die biometrischen Daten eines erheblichen Prozentsatzes der örtlichen Bevölkerung in einer Datenbank gespeichert werden, bis sämtliche Ermittlungen beendet sind – also für einen Zeitraum, der sich auf mehrere Jahre belaufen könnte.

Da die Tatortdatenbank nicht auf Bilder beschränkt ist, bei denen die Verhältnismäßigkeitsanforderungen erfüllt sind, ist die Zahl der abgleichbaren Bilder unbeschränkt. Dies widerspricht dem Grundsatz der Datenminimierung. Bei einer kleineren Menge von Bildern wären auch nicht-algorithmische und weniger stark eingreifende Mittel einsetzbar, z. B. Super Recognizer.[88]

Da das Beispiel aus dem Umfeld eines Protestaufzugs stammt, geben die Bilder wahrscheinlich auch Aufschluss über die politischen Meinungen der Demonstrationsteilnehmer; dies ist die zweite besondere Datenkategorie, die in diesem Szenario betroffen ist. Bei diesem Szenario ist nicht klar, wie sich die Erhebung dieser Daten vermeiden lässt und welche Garantien es gibt. Wenn betroffene Personen erfahren, dass ihre biometrischen Daten wegen ihrer Teilnahme an der Demonstration in die Polizeidatenbank aufgenommen wurden, kann sie dies zudem stark davor abschrecken, künftig von ihrem Recht auf Versammlungsfreiheit Gebrauch zu machen.

Die biometrischen Templates in der Datenbank können auch untereinander abgeglichen werden. So ist es der Polizei nicht nur möglich, ihr gesamtes Material nach einer bestimmten Person zu durchsuchen, sondern sie kann sogar für einen Zeitraum von mehreren Tagen das Verhaltensmuster einer Person nachvollziehen. Sie kann auch zusätzliche Informationen über Personen sammeln, zum Beispiel deren soziale Kontakte und politisches Engagement.

Weiter verstärkt wird der Eingriff durch den Umstand, dass die Daten ohne Wissen der betroffenen Personen verarbeitet werden.

Wenn man bedenkt, dass Menschen ständig Foto- und Videoaufnahmen machen und dass auch die Aufnahmen der allgegenwärtigen Videoüberwachungsanlagen biometrisch analysiert werden können, kann dies zu einer erheblichen abschreckenden Wirkung führen.

Bedenklich ist auch die umfangreiche Nutzung privater Fotos und Videos, bei denen auch die Gefahr von Missbrauch wie Denunziation besteht. Missbräuchliche Verwendung wie im Falle der Denunziation ist eine Gefahr, die bei Strafverfahren stets gegeben ist. Diese Gefahr ist aber wegen der Skalierbarkeit der verarbeiteten Datenmengen und der Zahl der Personen, um die es geht, erheblich erhöht; schließlich kann es vorkommen, dass Menschen Material über eine ihnen missliebige bestimmte Person oder Gruppe hochladen. Polizeiliche Aufrufe zum Hochladen von Fotos und Videos können dazu führen, dass Menschen diesen Aufrufen sehr leicht nachkommen können, insbesondere wenn ihnen dies anonym möglich ist, ohne eine Polizeidienststelle aufsuchen und sich ausweisen zu müssen.

3.4. Ergebnis

In diesem Beispiel gibt es keine spezifische Bestimmung, die als Rechtsgrundlage dienen könnte. Doch selbst wenn es eine Rechtsgrundlage gäbe, wären die Anforderungen an Erforderlichkeit und Verhältnismäßigkeit nicht erfüllt. Der Eingriff in die in der Charta verankerten Rechte der betroffenen Person auf Achtung des Privatlebens und den Schutz personenbezogener Daten wäre also unverhältnismäßig.

[88] Super Recognizer sind Menschen mit besonders guter Gesichtserkennungsfähigkeit. Vgl. auch: Face Recognition by Metropolitan Police Super-Recognisers, 26. Feb. 2016, DOI: 10.1371/journal.pone.0150036, https://pubmed.ncbi.nlm.nih.gov/26918457/.

4 SZENARIO 4

4.1. Beschreibung

Die Polizei implementiert eine Methode dafür, einer schweren Straftat verdächtige Personen, die von einer Videoüberwachungsanlage gefilmt wurden, durch nachträglich eingesetzte Gesichtserkennungstechnologie zu identifizieren. Im Rahmen von Vorermittlungen wählt ein Beamter manuell eines oder mehrere Bilder verdächtiger Personen aus dem am Tatort oder anderswo aufgezeichneten Videomaterial aus und sendet diese(s) an die forensische Abteilung. Die forensische Abteilung verwendet Gesichtserkennungstechnologie, um diese(s) Bild(er) mit Bildern von Personen abzugleichen, die von der Polizei in einer Datenbank gesammelt wurden (es handelt sich um eine sogenannte Beschreibungsdatenbank mit Personenbeschreibungen für Tatverdächtige und verurteilte Straftäter). Die Beschreibungsdatenbank wird für dieses Verfahren – vorübergehend und in isolierter Umgebung – mit Gesichtserkennungstechnologie analysiert, um den Abgleich durchführen zu können. Um möglichst wenig in die Rechte und Belange der abgeglichenen Personen einzugreifen, ist es nur einer sehr geringen Anzahl der Mitarbeiter der forensischen Abteilung gestattet, den eigentlichen Abgleich durchzuführen. Der Zugang zu den Daten ist auf diejenigen Beamten beschränkt, die mit der Bearbeitung der betreffenden Datei betraut sind. Zudem werden die Ergebnisse einer manuellen Ergebniskontrolle unterzogen, bevor sie an den Ermittlungsbeamten weitergeleitet werden. Eine Weiterleitung biometrischer Daten an Stellen außerhalb der kontrollierten isolierten Umgebung findet nicht statt. Im Ermittlungsverfahren werden dann lediglich das Ergebnis und das Bild (keine biometrischen Templates) verwendet. Die Mitarbeiter erhalten eine spezielle Schulung über die für diese Verarbeitung geltenden Vorschriften und Verfahren und die gesamte Verarbeitung personenbezogener und biometrischer Daten ist im nationalen Recht hinreichend geregelt.

Informationsquelle:

- Arten betroffener Personen: ☒ anhand von Aufnahmen aus Videoüberwachungsanlagen identifizierte Tatverdächtige
- Bildquelle: ☒ frei zugängliche Flächen/Räume ☒ Internet
- Bezug zur Straftat: ☒ unmittelbarer zeitlicher Bezug
  ☒ unmittelbarer räumlicher Bezug
- Art der Informationserfassung: ☒ aus der Ferne
- Kontext – Eingriff in andere Grundrechte: Ja, nämlich: ☒ Versammlungsfreiheit ☒ Meinungsäußerungsfreiheit ☒ verschiedene: __

Referenzdatenbank (für den Abgleich der erfassten Informationen):

- Spezifizität: ☒ spezifische Datenbanken für den Kriminalitätsbereich

Algorithmus:

- Art der Verarbeitung: ☒ One-to-Many-Identifikation

Ergebnis:

- Auswirkungen: ☒ Unmittelbar (z. B. Festnahme, Vernehmung der betroffenen Person)
- Automatisierte Entscheidung: ☒ NEIN

Rechtliche Prüfung:

- Einschlägiger rechtlicher Rahmen: ☒ Besondere nationale Rechtsvorschriften für die Verarbeitung (Gesichtserkennung) durch diese zuständige Behörde

4.2. Einschlägiger rechtlicher Rahmen

Bei diesem Szenario sieht das nationale Recht vor, dass biometrische Daten für forensische Analysen verwendet werden dürfen, soweit dies unbedingt erforderlich ist, um Personen, die einer schweren Straftat verdächtig sind, durch einen Abgleich mit Bildern in der Beschreibungsdatenbank zu identifizieren. Das nationale Recht bestimmt, welche Daten verarbeitet werden dürfen, und regelt auch die Verfahren für die Wahrung der Integrität und Vertraulichkeit personenbezogener Daten sowie die Verfahren für deren Löschung; damit bietet es hinreichende Garantien im Hinblick auf das Risiko von Missbrauch und Willkür.

4.3. Erforderlichkeit und Verhältnismäßigkeit

Auf forensischer Ebene ist der Einsatz von Gesichtserkennung offensichtlich zeiteffizienter als der manuelle Abgleich. Weil die Bildauswahl vorab manuell vorgenommen wird, ist der Eingriff weniger stark, als es bei einem Datenbankabgleich des gesamten Videomaterials der Fall wäre; auf diese Weise wird differenziert und die Maßnahme wird gezielt auf Personen beschränkt, bei denen das Ziel – die Bekämpfung schwerer Straftaten – gegeben ist. Dennoch ist es aber wichtig, zu prüfen, ob im Einzelfall der Abgleich innerhalb angemessener Zeit manuell erfolgen kann. Werden der Personenkreis, dem der Zugang zur Technologie gestattet ist, und die personenbezogenen Daten eingeschränkt, sind die Auswirkungen auf die Rechte auf Schutz der Privatsphäre und Datenschutz weniger stark; dies ist auch der Fall, wenn die biometrischen Templates weder gespeichert noch im weiteren Verlauf der Ermittlungen verwendet werden. Bei manueller Kontrolle des Ergebnisses ist auch die Gefahr von Falschtreffern geringer.

4.4. Ergebnis

Es ist wichtig, dass das nationale Recht nicht nur für die Verarbeitung biometrischer Daten eine hinreichende Rechtsgrundlage vorsieht, sondern auch für die nationale Datenbank, mit der der Abgleich vorgenommen wird. Bei diesem Szenario wurden mehrere Vorkehrungen getroffen, um den Eingriff in die Datenschutzrechte in Grenzen zu halten: die in der Rechtsgrundlage geregelten Voraussetzungen für die Verwendung der Gesichtserkennungstechnologie, die Anzahl der Personen, die Zugang zur Technologie und den biometrischen Daten haben, manuelle Kontrollen usw. Mit der Gesichtserkennungstechnologie ist die Ermittlungsarbeit der forensischen Abteilung der Polizei wesentlich effizienter. Außerdem beruht ihr Einsatz auf einem Gesetz, das der Polizei die Verarbeitung biometrischer Daten gestattet, soweit diese unbedingt erforderlich ist. Innerhalb dieser Grenzen kann der Einsatz als rechtmäßiger Eingriff in die Rechte der Person angesehen werden.

5 SZENARIO 5

5.1. Beschreibung

Biometrische Fernidentifizierung liegt vor, wenn die Identität von Personen mittels biometrischer Identifikatoren (Merkmale wie Gesichtsbild, Gangbild, Iris usw.) aus der Ferne festgestellt wird; dies kann im öffentlichen Raum und in ununterbrochener oder fortlaufender Weise geschehen, indem diese Merkmale mit in einer Datenbank gespeicherten (biometrischen) Daten abgeglichen werden[89]. Die biometrische Fernidentifizierung ist in Echtzeit möglich, sofern die Erfassung des Bildmaterials, der Abgleich und die Identifikation ohne größere zeitliche Verzögerung erfolgen.

Vor jedem Einsatz biometrischer Fernidentifizierung in Echtzeit erstellt die Polizei eine Beobachtungsliste der für ihr Ermittlungsverfahren relevanten Personen. Die Liste wird mit

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

Gesichtsbildern der Personen populiert. Bei Hinweisen, dass sich die Personen an einem bestimmten Ort aufhalten werden (z. B. in einem Einkaufszentrum oder auf einem öffentlichen Platz), entscheidet die Polizei, ob, wo und wie lange sie die biometrische Fernidentifizierung einsetzt.

Am Einsatztag wird ein als Kontrollzentrum dienender Polizeiwagen vor Ort geparkt, der mit einem erfahrenen Polizeibeamten besetzt ist. In diesem Polizeiwagen gibt es Monitore, auf denen das Bildmaterial aus den Videoüberwachungsanlagen zu sehen ist, die ad hoc oder dauerhaft dort installiert sind. Mit der Technologie werden die Gesichtsbilder der an den Kameras vorbeigehenden Passanten isoliert, in ein biometrisches Template umgewandelt und dann mit den biometrischen Templates auf der Beobachtungsliste abgeglichen.

Eine potenzielle Übereinstimmung eines der Passanten mit einer Person auf der Beobachtungsliste wird den Beamten im Polizeiwagen gemeldet, die dann ggf. die Beamten vor Ort über den Treffer verständigen, z. B. per Sprechfunk. Der Beamte vor Ort prüft dann, ob er eingreift, sich der Person nähert oder sie letztendlich festnimmt. Die vom Beamten vor Ort ergriffenen Maßnahmen werden aufgezeichnet. Handelt es sich um eine diskrete Überprüfung (etwa zur Feststellung, mit wem die Person unterwegs ist, welche Kleidung sie trägt und wohin sie sich bewegt), werden die Informationen gespeichert.

Das zugrundegelegte nationale Gesetz enthält eine allgemeine Bestimmung, nach der die Verarbeitung biometrischer Daten für die Zwecke der eindeutigen Identifikation einer natürlichen Person zulässig ist, sofern diese unbedingt erforderlich ist und geeignete Garantien für die Rechte und Freiheiten der betroffenen Person gegeben sind.

<u>Informationsquelle:</u>

- Arten betroffener Personen: ☒ alle Personen
- Bildquelle: ☒ frei zugängliche Flächen/Räume
- Bezug zur Straftat: ☒ Nicht notwendigerweise unmittelbarer räumlicher oder zeitlicher Bezug
- Art der Informationserfassung: ☒ aus der Ferne
- Kontext – Eingriff in andere Grundrechte: Ja, nämlich: ☒ Versammlungsfreiheit ☒ Meinungsäußerungsfreiheit ☒ Verschiedene
- Etwaige zusätzliche Informationsquellen bezüglich der betroffenen Person:
  ☒ sonstige: nicht ausgeschlossen (etwa Benutzung von Geldautomaten oder aufgesuchte Geschäfte)

<u>Referenzdatenbank (für den Abgleich der erfassten Informationen)</u>:

- Spezifizität: ☒ spezifische Datenbanken für den Kriminalitätsbereich

<u>Algorithmus:</u>

- Art der Verarbeitung: ☒ One-to-Many-Identifikation

<u>Ergebnis:</u>

- Auswirkungen: ☒ Unmittelbar (z. B. Festnahme, Vernehmung der betroffenen Person)
- Automatisierte Entscheidung: ☒ NEIN
- Speicherfrist: bis alle in Betracht kommenden Ermittlungen beendet sind

<u>Rechtliche Prüfung:</u>

- Art der Vorabinformation der betroffenen Person: ☒ Allgemeine Informationen auf der Website der Strafverfolgungsbehörde

- Einschlägiger rechtlicher Rahmen: ☒ JI-Datenschutzrichtlinie weitgehend wortgleich ins nationale Recht übernommen ☒ Allgemeines nationales Gesetz für die Verwendung biometrischer Daten durch Strafverfolgungsbehörden

5.2. Einschlägiger rechtlicher Rahmen

Rechtsgrundlagen, die lediglich die Generalklausel in Artikel 10 der JI-Datenschutzrichtlinie wiederholen, sind nicht hinreichend deutlich formuliert, den natürlichen Personen angemessen Aufschluss darüber zu geben, unter welchen Voraussetzungen und Umständen Strafverfolgungsbehörden befugt sind, Aufzeichnungen aus Videoüberwachungsanlagen im öffentlichen Raum dazu zu verwenden, ein biometrisches Template des Gesichts der Person anzufertigen und dieses mit Polizeidatenbanken abzugleichen. Der in diesem Szenario gegebene rechtliche Rahmen genügt deshalb nicht den Mindestanforderungen an eine Rechtsgrundlage.[90]

5.3. Erforderlichkeit und Verhältnismäßigkeit

Die Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit sind umso höher, je schwerer der Eingriff ist. Die biometrische Fernidentifizierung im öffentlichen Raum hat Auswirkungen auf mehrere Grundrechte:

Bei derartigen Szenarien wird jeder einzelne Passant im betreffenden öffentlichen Raum überwacht. Sie berühren also in hohem Maße die berechtigte Erwartung der Bevölkerung, sich im öffentlichen Raum anonym bewegen zu können[91]. Diese Erwartung ist für viele Aspekte des demokratischen Lebens unerlässlich: etwa für die Entscheidung, sich einer Bürgervereinigung anzuschließen, an Versammlungen teilzunehmen und mit Menschen der verschiedensten gesellschaftlichen und kulturellen Hintergründe zusammenzutreffen, an politischem Protest teilzunehmen oder Orte jeglicher Art aufzusuchen. Das Konzept der Anonymität im öffentlichen Raum ist von zentraler Bedeutung dafür, Informationen und Ideen frei sammeln und austauschen zu können. Dieses Konzept schützt die Meinungsvielfalt, die Freiheit, sich friedlich zu versammeln, die Vereinigungsfreiheit und den Schutz von Minderheiten und untermauert die Grundsätze der Gewaltenteilung und der gegenseitigen Gewaltenkontrolle. Wird das Konzept der Anonymität im öffentlichen Raum untergraben, so kann dies starke abschreckende Wirkung auf die Bürger haben und sie vor bestimmten Verhaltensweisen, die ihnen in einer freien und offenen Gesellschaft zweifellos zustehen, zurückscheuen lassen. Damit wäre das Gemeinwohl berührt, denn für eine demokratische Gesellschaft ist die Selbstbestimmung der Bürger und deren Teilhabe am demokratischen Prozess erforderlich.

Wird eine solche Technologie eingesetzt, so werden bei jedem Gang in dem der Überwachung unterliegenden Bereich – ob beim Spaziergang die Straße entlang, beim Gang zur U-Bahn oder zur Bäckerei – personenbezogene, auch biometrische Daten, von Strafverfolgungsbehörden erfasst; im ersten Szenario werden diese Daten auch mit Polizeidatenbanken abgeglichen. Eine Situation, bei der im selben Umfang Fingerabdrücke abgenommen würden, wäre offensichtlich unverhältnismäßig.

[90] In Fällen, in denen für ein wissenschaftliches Projekt zur Erforschung der Verwendung von Gesichtserkennungstechnologie personenbezogene Daten verarbeitet werden müssten, diese Verarbeitung jedoch nicht unter Artikel 4 Absatz 3 der JI-Datenschutzrichtlinie fiele oder außerhalb des Anwendungsbereichs des Unionsrechts läge, wäre die DSGVO anwendbar. Im Falle von Pilotprojekten, an die sich Strafverfolgungsmaßnahmen anschlössen, wäre die JI-Datenschutzrichtlinie weiterhin anwendbar.

[91] Antwort des EDSA an die Mitglieder des Europäischen Parlaments hinsichtlich der von Clearview AI entwickelten Gesichtserkennungs-App, Schreiben vom 10. Juni 2020, Akt.Z.: OUT2020-0052.

Die Zahl der betroffenen Personen ist äußerst hoch, da jeder, der den betreffenden öffentlichen Bereich passiert, betroffen ist. Hinzu kommt noch, dass diese Szenarien mit automatisierter Massenverarbeitung biometrischer Daten und dem Massenabgleich biometrischer Daten mit Polizeidatenbanken verbunden wären.

Massenüberwachung ist nach der europäischen Rechtsprechung durchweg verboten (so hat der EGMR in der Rechtssache S. and Marper v. UK entschieden, dass die unterschiedslose Speicherung biometrischer Daten einen „unverhältnismäßigen Eingriff" in das Recht auf Privatsphäre darstellt, weil sie nicht als „in einer demokratischen Gesellschaft notwendig" angesehen wird).

Biometrische Fernidentifizierung kommt der Massenüberwachung insofern recht nahe, als es keine zuverlässigen Einschränkungsmöglichkeiten gibt. Sie unterscheidet sich wesentlich von der reinen Videoüberwachung, da zwar bereits die mögliche Nutzung von Videomaterial ohne biometrische Identifikation einen starken Eingriff darstellt, dieser sich jedoch in Grenzen hält. Wird dagegen Gesichtserkennungstechnologie angewendet, so werden dadurch die bereits weit verbreiteten Videoüberwachungssysteme, die als hauptsächliche Datenquelle dienen, eine ganz andere Qualität annehmen. Insbesondere im Hinblick auf die sich ergebende Abschreckungswirkung ist zu beachten, dass die möglichen Einschränkungen der Anwendung bereits bestehender Videoüberwachungsanlagen nicht sichtbar sein werden, weshalb die Öffentlichkeit ihnen nicht trauen wird.

Bei biometrischer Fernidentifizierung durch die Polizei wird jeder Mensch als potenzieller Verdächtiger behandelt. In einem Rechtsstaat ist jedoch – bis zum Beweis des Gegenteils – grundsätzlich von der Unschuld der Bürger auszugehen. Dieser Grundsatz spiegelt sich zum Teil auch in der JI-Datenschutzrichtlinie, wo hervorgehoben wird, dass es notwendig ist, zu unterscheiden zwischen der Behandlung von verurteilten Personen oder Tatverdächtigen, bei denen für die Strafverfolger „*ein begründeter Verdacht besteh[en muss], dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden*" (Artikel 6 Buchstabe a der JI-Datenschutzrichtlinie), und denjenigen, die weder einer Straftat wegen verurteilt wurden noch einer solchen verdächtig sind.

Wenden Strafverfolgungs- oder Ordnungsbehörden an Verkehrsknotenpunkten oder im öffentlichen Raum eine Technologie an, mit der eine Einzelperson eindeutig identifiziert werden kann, und werden deren Aufenthalt und Bewegungen verfolgt und analysiert, so treten dabei die sensibelsten Informationen über die Person zutage (selbst sexuelle Präferenzen, Religion, Gesundheitsprobleme). Damit einher geht das enorme Risiko unrechtmäßigen Datenzugangs und unrechtmäßiger Datennutzung.

Wird ein System zur Erfassung von Verhalten und persönlichen Eigenschaften installiert, das Aufschluss über den Kernbereich der Persönlichkeit gibt, so hat das starke abschreckende Wirkung. Wenn Menschen deswegen davor zurückscheuen, sich Protestveranstaltungen anzuschließen, schadet das dem demokratischen Prozess. Mancher würde vielleicht auch davor zurückscheuen, sich mit gewissen Freunden zu treffen oder in der Öffentlichkeit sehen zu lassen, von denen er weiß, dass sie polizeiauffällig wurden oder sich auffällig verhalten, weil zu befürchten wäre, damit die Aufmerksamkeit des System-Algorithmus – und folglich der Strafverfolgungsbehörden – auf sich zu lenken.

Es ist unmöglich, vulnerable betroffene Personen wie etwa Kinder zu schützen. Auch bestimmte Personengruppen mit beruflichem Interesse an der Geheimhaltung ihrer Kontakte, etwa Journalisten, Rechtsanwälte und Geistliche, die häufig auch entsprechenden Berufspflichten unterliegen, sind betroffen. Es könnte zum Beispiel dazu kommen, dass die Quelle und der Journalist oder aber der Umstand, dass jemand einen Strafverteidiger aufsucht, bekannt würde. Das Problem gilt nicht nur für

irgendwelche öffentlichen Orte, wo sich z. B. Journalisten mit ihren Quellen treffen, sondern natürlich auch für die Teile des öffentlichen Raums, die durchquert werden müssen, um Einrichtungen zu betreten oder Berufsangehörige aufzusuchen.

Menschen, die mit der Gesichtserkennungstechnologie nicht einverstanden sind, werden vielleicht ihr Verhalten ändern, um Orte, an denen Gesichtserkennungstechnologie eingesetzt wird, zu meiden und sich dadurch aus dem gesellschaftlichen Leben und kulturellen Veranstaltungen zurückziehen. Je nachdem, inwieweit Gesichtserkennungstechnologie eingesetzt wird, können die Auswirkungen auf die Menschen so stark sein, dass sie in ihrer Fähigkeit, ein menschenwürdiges Leben zu führen, beeinträchtigt sind[92].

Es ist deshalb sehr wahrscheinlich, dass hier das Wesen – der unantastbare Kern – des Rechts auf den Schutz personenbezogener Daten berührt ist. Starke Anzeichen (vgl. Abschnitt 3.1.3.2 der Leitlinien) dafür ergeben sich insbesondere aus folgenden Umständen: Die Strafverfolgungsbehörden verarbeiten automatisch und in großem Maßstab einzigartige biologische Merkmale von Menschen, und zwar mittels auf Plausibilität beruhender Algorithmen, deren Ergebnisse nur eingeschränkt erklärbar sind. Die Einschränkung der Rechte auf Privatsphäre und Datenschutz erfolgt ohne Rücksicht auf das individuelle Verhalten der Person oder ihre Umstände. Statistisch sind fast alle von diesem Eingriff betroffenen Personen gesetzestreue Bürger. Es gibt nur eingeschränkte Möglichkeiten, die betroffenen Personen zu unterrichten. In den meisten Fällen wird der Rechtsweg erst anschließend beschritten werden können.

Das Vertrauen auf ein System, das auf Plausibilität beruht und nur eingeschränkt erklärbar ist, kann zu Haftungsdiffusion führen, fehlende Rechtsbehelfe können zu fahrlässigem Vorgehen verleiten.

Wird ein solches System, das sich auch auf bestehende Videoüberwachungsanlagen anwenden lässt und mit wenig Aufwand und ohne, dass dies für andere ersichtlich ist, eingesetzt werden kann, erst angewendet, so kann es dazu missbraucht werden, systematisch und in kürzester Zeit Personen nach deren ethnischer Herkunft, Geschlecht, Religion usw. aufzulisten. Bei dem bereits praktizierten Prinzip, personenbezogene Daten nach vorab festgelegten Kriterien wie dem Aufenthaltsort einer Person und ihrem Reiseweg zu verarbeiten[93], kann es leicht zu Diskriminierung kommen.

Je nach Sensibilität, Aussagekraft und Menge der verarbeiteten Daten besteht bei Systemen für die Ferngesichtserkennung an öffentlich zugänglichen Orten die Gefahr, dass diese zum Nachteil der betroffenen Einzelpersonen missbraucht werden. Derartige Daten können auch leicht gesammelt und missbraucht werden, um Personen wie zum Beispiel Mitglieder der politischen Opposition, Beamte oder Journalisten, die entscheidend zur wechselseitigen Kontrolle im Rahmen der Gewaltenteilung beitragen, unter Druck zu setzen.

Als Letztes ist noch zu bedenken, dass Gesichtserkennungssysteme zu starken Verzerrungseffekten in Bezug auf Rasse und Geschlecht neigen: Falsche Treffer kommen überproportional häufig bei

---

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

93 Vgl. Artikel 6 der Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität und Artikel 33 der Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226.

Menschen mit dunklerer Hautfarbe und weiblichen Personen[94] vor, was zu Diskriminierung führt. Die Stigmatisierung dieser Gruppen wird durch auf falsche Treffer hin ergriffene polizeiliche Maßnahmen wie Durchsuchungen und Festnahmen noch verstärkt.

5.4. Ergebnis

Den vorgenannten Szenarien, bei denen es um die Fernverarbeitung biometrischer Daten im öffentlichen Raum geht, fehlt eine angemessene Abwägung zwischen konkurrierenden privaten und öffentlichen Interessen; es handelt sich deshalb um einen unverhältnismäßigen Eingriff in die in den Artikeln 7 und 8 der Charta verankerten Rechte der betroffenen Person.

6 SZENARIO 6

6.1. Beschreibung

Ein Privatunternehmen bietet eine App an, bei der Gesichtsbilder aus dem Internet gescrapt werden, um daraus eine Datenbank anzulegen. Der Nutzer, z. B. die Polizei, kann ein Bild hochladen und die App versucht dann mittels biometrischer Identifikation, dieses Bild mit den Gesichtsbildern oder biometrischen Templates in ihrer Datenbank abzugleichen.

Eine örtliche Polizeidienststelle ermittelt wegen einer Straftat, die auf Video aufgezeichnet wurde, bei der jedoch mehrere potenzielle Zeugen und Tatverdächtige nicht durch den Abgleich der in den eigenen Datenbanken gesammelten Informationen oder durch sonstige Informationskanäle identifiziert werden können. Nach dem derzeitigen Informationsstand sind die Personen in keiner bestehenden Polizeidatenbank registriert. Die Polizei beschließt, das oben beschriebene, von einem Privatunternehmen angebotene Tool zu benutzen, um die Personen mittels biometrischer Identifikation zu identifizieren.

Informationsquelle:

- Arten betroffener Personen: ☒ Alle Bürger (Zeugen) ☒ Verurteilte Straftäter ☒ Tatverdächtige
- Bildquelle: ☒ Im Rahmen der Vorermittlungen an einem öffentlichen Ort oder anderswo gesammelte Videoaufnahmen
- Bezug zur Straftat: ☒ nicht erforderlich
- Art der Informationserfassung: ☒ Fernerfassung
- Kontext – Eingriff in andere Grundrechte: Ja, nämlich: ☒ Versammlungsfreiheit ☒ Meinungsäußerungsfreiheit ☒ Verschiedene: __

Referenzdatenbank (für den Abgleich der erfassten Informationen):

- Spezifizität: ☒ aus dem Internet populierte Allgemeinzweckdatenbanken

Algorithmus:

- Art der Verarbeitung: ☒ One-to-Many-Identifikation

Ergebnis:

- Auswirkungen ☒ unmittelbar (z. B. die betroffene Person wird festgenommen und vernommen, diskriminierendes Verhalten)
- Automatisierte Entscheidung: ☒ NEIN

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

Rechtliche Prüfung:

- Art der Vorabinformation der betroffenen Person: ☒ Nein

6.2. Einschlägiger rechtlicher Rahmen

Wenn ein Privatunternehmen einen Dienst anbietet, der eine Verarbeitung personenbezogener Daten einschließt, deren Zweck und Mittel das Privatunternehmen festlegt (in diesem Fall das Scraping von Bildern im Internet für den Aufbau einer Datenbank), so muss es für diese Verarbeitung durch das Privatunternehmen eine Rechtsgrundlage geben. Des Weiteren muss die Strafverfolgungsbehörde, die sich dafür entscheidet, diesen Dienst für ihre Zwecke zu nutzen, für die Verarbeitung, deren Zwecke und Mittel sie festlegt, eine Rechtsgrundlage haben. Die Strafverfolgungsbehörde ist nur dann zur Verarbeitung biometrischer Daten befugt, wenn es einen rechtlichen Rahmen gibt, in dem das Ziel, die zu verarbeitenden personenbezogenen Daten, die Zwecke der Verarbeitung und die Verfahren für die Wahrung der Integrität und Vertraulichkeit der personenbezogenen Daten sowie die Verfahren für deren Löschung geregelt sind.

Dieses Szenario ist mit der Massenerfassung personenbezogener Daten von Personen verbunden, die keine Kenntnis davon haben, dass ihre Daten erfasst werden. Eine solche Verarbeitung könnte nur unter sehr außergewöhnlichen Umständen rechtmäßig sein. Je nachdem, wo sich die Datenbank befindet, könnte ein solcher Dienst auch mit der Übermittlung personenbezogener Daten und/oder besonderer Kategorien personenbezogener Daten in Länder außerhalb der Europäischen Union einhergehen (z. B., wenn die Polizei das im Überwachungsvideo oder auf andere Weise erfasste Gesichtsbild „sendet“). In einem solche Fall ist die Übermittlung an die in Artikel 39 der JI-Datenschutzrichtlinie genannten besonderen Voraussetzungen geknüpft.

In diesem Szenario gibt es keine besonderen Vorschriften, die diese Verarbeitung durch die Strafverfolgungsbehörde gestatten.

6.3. Erforderlichkeit und Verhältnismäßigkeit

Die Nutzung dieses Dienstes durch die Strafverfolgungsbehörde bedeutet, dass personenbezogene Daten mit einem Privatunternehmen geteilt werden, das eine Datenbank verwendet, in der personenbezogene Daten uneingeschränkt und massenhaft erfasst werden. Es gibt keinen Zusammenhang zwischen den erfassten personenbezogenen Daten und dem von der Strafverfolgungsbehörde verfolgten Ziel. Der Datenaustausch zwischen der Strafverfolgungsbehörde und dem Privatunternehmen bedeutet auch, dass der Behörde die Kontrolle über die von dem Privatunternehmen verarbeiteten Daten fehlt und dass es für die betroffenen Personen sehr schwierig ist, ihre Rechte auszuüben, da sie keine Kenntnis davon haben werden, dass ihre Daten auf diese Weise verarbeitet werden. Deshalb kann eine solche Verarbeitung nur in Ausnahmesituationen und unter allerstrengsten Voraussetzungen stattfinden. Es ist fraglich, ob es ein Ziel gibt, das die in der Richtlinie genannten Anforderungen erfüllen würde, da alle Ausnahmen von den Rechten auf Privatsphäre und Datenschutz und auch alle Einschränkungen dieser Rechte nur anwendbar sind, soweit dies unbedingt erforderlich ist. Das allgemeine Interesse an einer wirksamen Bekämpfung schwerer Straftaten ist für sich genommen nicht geeignet, eine Verarbeitung zu rechtfertigen, für die solche enormen Datenmengen unterschiedslos gesammelt werden. Diese Verarbeitung würde deshalb den Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit nicht genügen.

6.4. Ergebnis

Da es an klaren, genauen und vorhersehbaren Vorschriften fehlt, die den Anforderungen in Artikel 4 und 10 der Richtlinie genügen, und es ist keinen Nachweis dafür gibt, dass diese Verarbeitung zum Erreichen der verfolgten Ziele unbedingt erforderlich ist, ist der Schluss zu ziehen, dass die Verwendung dieser App den Anforderungen an die Erforderlichkeit und Verhältnismäßigkeit nicht genügen würde und dass sie einen unverhältnismäßigen Eingriff in die in der Charta verankerten Rechte der betroffenen Personen auf den Schutz ihrer Privatsphäre und personenbezogenen Daten darstellen würde.