HUMBOLDT FORUM RECHT
- Die juristische Internet-Zeitschrift an der Humboldt-Universität zu Berlin -

HFR 7/2012 ISSN 1862-7617 Aufsatz

Dr. Moritz Karg, Hamburg

Biometrische Verfahren zur Gesichtserkennung und Datenschutz in Sozialen Netzwerken*

Der Beitrag von Dr. Karg befasst sich mit datenschutzrechtlichen Fragestellungen bei biometrischen Verfahren zur Gesichtserkennung in sozialen Netzwerken. Ausgehend von einer Darstellung der technischen Grundlagen und der Funktionsweise der Gesichtserkennung wendet sich der Autor dem Gefährdungspotenzial des Einsatzes biometrischer Erkennungsmethoden zu, so dass auch der mit der Materie nicht vertraute Leser/die Leserin schnell Zugang zur datenschutzrechtlichen Relevanz biometrischer Verfahren zur Gesichtserkennung findet. Bei der in sich schlüssigen Prüfung der datenschutzrechtlichen Zulässigkeit gelangt der Autor zu dem Ergebnis, dass die derzeit geltenden gesetzlichen Erlaubnistatbestände nicht geeignet sind, Verfahren der biometrischen Gesichtserkennung zu legitimieren.

I. Einleitung

1 Facebook tut es, Google+ auch und das gesamte Geschäftsmodell von face.com basierte darauf – das Verfahren zur Gesichtserkennung. Die genannten Dienste stehen beispielhaft für einen Trend, der sich außerhalb und innerhalb sozialer Netzwerke immer stärker durchsetzt. Es handelt sich um Verfahren zur biometrischen Erfassung von Gesichtern auf digitalen Bildern. Die Versuche Personen auf Bildern zu identifizieren, sind nicht neu. Bereits in den vergangenen Jahren fanden immer wieder Modellprojekte statt, z.B. Personen auf Videoaufnahmen automatisiert zu erkennen.[1] Das Ziel derartiger Versuche war klar. Es sollten z.B. gesuchte Personen automatisiert erkannt werden. Die Vorteile für eine effektive Strafverfolgung liegen auf der Hand. Die Technologie war jedoch nicht ausgereift und produzierte zu viele „false positives“[2], d.h. die Systeme erkannten die falschen Personen als Richtige.[3] Die Ausbreitung der Technologie schreitet dennoch weiter voran. Biometrisch vermessene Bilder kommen u.a. bei der Ausstellung von amtlichen Identifikationsdokumenten, z.B. Reispässen zur Anwendung.[4]

2 Mittlerweile sind kommerzielle Anbieter vor allem im Bereich der sozialen Medien in die Entwicklung und Nutzung biometrischer Erkennungsverfahren eingestiegen oder ergänzen ihre Angebote dahingehend.[5] Für staatliche Stellen steht hauptsächlich die Sicherheit der Identitätsfeststellung, die Echtheit ausgestellter Dokumente und damit einhergehend die Wahrung der staatlichen Sicherheit im Vordergrund.[6] Privatwirtschaftliche Verwender dieser Technologie fokussieren vielmehr auf die nutzerfreundlichere Gestaltung ihrer Dienste.[7] Das Kalkül der Anbieter scheint zu sein,

* Die in diesem Beitrag geäußerten Ansichten stellen ausschließlich die Privatmeinung des Autors dar.
[1] Siehe Forschungsprojekt des BKA „Foto-Fahndung“, https://www.bka.de/nn_196810/DE/ThemenABisZ/Forschung/FotoFahndung/fotoFahndung.html (18.07.2012).
[2] *Roßnagel/Hornung*, Biometrische Daten in Ausweisen, DuD 2005, 69, 70.
[3] http://www.heise.de/newsticker/meldung/BKA-2D-Foto-Fahndung-ist-nicht-einsatzfaehig-150068.html (18.07.2012).
[4] Art. 1 Verordnung (EG) Nr. 2252/2004.
[5] http://www.heise.de/newsticker/meldung/Facebook-kauft-Technik-fuer-Gesichtserkennung-1620544.html (18.07.2012).
[6] *Schaar*, Biometrische Reisekontrolle, MMR 2008, 137, 138; Erwägungsgrund 3 Verordnung (EG) Nr. 2252/2004.
[7] Vgl. Facebook, Beschreibung der Markierungsfunktion, https://www.facebook.com/help/?faq=122175507864081 (18.07.2012).

dass sich aus der vermeintlichen Nutzerfreundlichkeit der Dienste eine engere Bindung des Einzelnen an das Netzwerk ergibt. Letzteres wiederum soll in einer Wertsteigerung des gesamten Dienstes im Hinblick auf die Vermarktung des bestehenden Datenbestandes resultieren.

3 Den unbestreitbaren Vorteilen dieser Technologie stehen die fast schon auf der Hand liegenden Nachteile gegenüber. Je genauer die Erkennungsverfahren arbeiten und je verbreiteter deren Einsatz wird, desto mehr schwindet die auch in der Öffentlichkeit verfassungsrechtlich geschützte Anonymität[8]. Sie ist, neben dem Schutz des Einzelnen, maßgeblich für die ungehinderte Wahrnehmung demokratischer Grundrechte, wie dem Recht auf Versammlungsfreiheit, Art. 8 GG.[9]

4 Die weitere Entwicklung dieser Technologie und deren Einsatz lassen sich nicht aufhalten. Es ist somit erforderlich, die Rahmenbedingungen des Einsatzes zu beschreiben und sicherzustellen, dass diese effektiv durch- und umgesetzt werden.

5 II. Technische Grundlagen und Funktionsweise der Gesichtserkennung

Eine individuelle Beschreibung der biometrischen Verfahren einzelner Anbieter ist nicht erforderlich, da sich die Verfahren in den Grundstrukturen gleichen. Ausgangspunkt und Basisprozess ist jeweils die Vermessung des körperlichen Merkmals, die Erstellung des Templates und die daran anknüpfende Verwendung dieses Templates für den jeweiligen Zweck.[10] In Abhängigkeit von dem Einsatzzweck kann es angezeigt sein, in einem zweiten Teilverfahren diese Schritte temporär zu wiederholen, um einen Abgleich mit dem Ergebnis des Basisprozesses zu ermöglichen.

6 Auf der Grundlage eines fiktiven Gesichtserkennungsverfahrens zur Identifizierung von Personen auf digitalen Fotos innerhalb eines sozialen Netzwerkes soll das theoretische Modell beschrieben werden: Erster erforderlicher Schritt ist die Erstellung des dauerhaften Referenztemplates bzw. der Aufbau der biometrischen Datenbank. Das Referenztemplate wird auf der Grundlage eines von einem Nutzer oder einer Nutzerin zu dem Betreiber übermittelten digitalen Fotos erzeugt. Das System analysiert zuerst die Struktur und Informationen des Fotos und prüft, ob darauf mit einem Gesicht vergleichbare Strukturen erfasst werden können. Kann das System einen derartigen Bereich festlegen, erfolgt die eigentliche Auswertung der erkannten Struktur. Dazu wird das Gesicht vermessen. Typische Messpunkte sind Augen, Nase, Mund und Kinn. Der Abstand zwischen diesen und gegebenenfalls weiteren Messpunkten wird gemessen und daraus ein biometrisches Template erzeugt. Dieses ist in der Regel eine Zahl. Sie ist eindeutig und individualisiert das abgebildete Gesicht.

7 Das so erzeugte Template wird in einer Datenbank abgespeichert und muss nunmehr mit der Identität der abgebildeten Person verknüpft werden. In sozialen Netzwerken kann dies durch die Herstellung einer Relation zwischen Templateeintrag und dem Eintrag in der Profildatenbank erfolgen. Das so inhaltlich qualifizierte Template findet dann als Referenztemplate Verwendung. Voraussetzung für die zukünftige, erfolgreiche Nutzung des Referenztemplates ist, dass es der richtigen Person zugeordnet wird. Innerhalb sozialer Netzwerke kann dies relativ einfach erfolgen. Entweder andere Nutzerinnen und Nutzer identifizieren die Person auf dem Bild oder, was eine höhere Genauigkeit erzeugt, der Betroffene selbst „erkennt“ sich auf dem Bild und bestätigt dies.

[8] *BVerfG*, Beschl. v. 23.02.2007, 1 BvR 2368/06 vom 23.2.2007, Ziff. 39, http://www.bverfg.de/entscheidungen/rk20070223_1bvr236806.html (18.07.2012).
[9] *BVerfG*, Beschl. v. 17.2.2009, 1 BvR 2492/08, Ziff. 130f., http://www.bverfg.de/entscheidungen/rs20090217_1bvr249208.html (18.07.2012).
[10] *Gundermann/Probst*, Biometrie in: *Roßnagel* (Hrsg.), Handbuch des Datenschutzrechts, Kap. 96, Rn. 8ff.

8 Wird nach diesem Prozess erneut ein digitales Foto an den Betreiber übermittelt, wird erneut das Bild vermessen und wiederum ein Template erzeugt. Dieses wird dann mit dem Referenztemplates abgeglichen. Je nach dem Grad der Übereinstimmung sind dann verschiedene Reaktionen möglich. In der Praxis hat sich u.a. ein Verfahren etabliert, den Nutzern der Netzwerke das Ergebnis der Auswertung darzustellen. Diese sind dann in der Lage, den Abgleich inhaltlich zu prüfen und z.B. bei einer fehlerhaften Erkennung, das Ergebnis zu korrigieren. Der Vorteil der Anbieter bei diesem Verfahren ist, dass ohne eigenen Ressourcenaufwand der Auswertungsmechanismus qualitätsgesichert wird.

9 Das temporär erstellte Template wird bei lernfähigen Systemen zu dem bereits bestehenden Referenztemplate hinzugespeichert und verbessert darüber die Erkennungsquote bei zukünftigen Auswertungen. Je häufiger eine Erkennung erfolgt, desto genauer wird die korrekte Individualisierung der Person.

10 ## III. Gefährdungspotenzial des Einsatzes biometrischer Erkennungsmethoden

Der Einsatz biometrischer Erkennungsmaßnahmen steht unter einem erhöhten datenschutzrechtlichen Rechtfertigungsdruck.[11] Aus rechtspolitischer Sicht lässt sich dies vor allem mit zwei grundsätzlichen Bedenken gegen den Einsatz biometrischer Verfahren begründen.

S. 123

11 Zum einen birgt der Einsatz von Verfahren der digitalen Erfassung und Auswertung von Körpereigenschaften[12] die Gefahr der überschießenden Informationsvermittlung. So sind z.B. über die digitale Erfassung und Auswertung der Gesichtsphysiognomie Rückschlüsse auf Alter, Geschlecht oder ethnische Herkunft möglich.[13] Letztere Angaben gehören zu den besonderen personenbezogenen Daten, deren Verarbeitung nur unter gesonderten Voraussetzungen zulässig ist.[14] Teilweise wird sogar vertreten, dass sich mittels biometrischer Angaben Aussagen über den Gesundheitszustand einer Person treffen lassen.[15] Auch wenn Letzteres nicht unbestritten ist, wird der Kern der Gefährdung deutlich. Mit der Erfassung eines biometrischen Merkmals können über die Trägerin oder den Träger des Merkmals weitere Aussagen getroffen werden. Der potenzielle Umfang dieses Aussagegehaltes ist jedoch nicht unmittelbar transparent und hängt maßgeblich von der eingesetzten Technologie und Erhebungsqualität ab. Während Betroffene den Aussagegehalt z.B. einer E-Mailadresse abschätzen können, ist eine derartige Risikobewertung bei der digitalen Auswertung von Körpereigenschaften nicht ohne weiteres möglich. Biometrische Merkmale sind, wie z.B. der Fingerabdruck oder die Gesichtsphysiognomie, willentlich kaum änderbar.

12 Die zweite potentielle Gefährdung für die Persönlichkeitsrechte besteht in der Schaffung und Verwendung eines unveränderlichen, individuellen, digitalen Referenzmerkmals. Über dieses ist die Trägerin oder der Träger des ausgewerteten Körpermerkmals jederzeit individualisierbar. Körpermerkmale sind in der Regel nicht bzw. nur sehr schwer änderbar. Die heute eingesetzten Systeme erlauben eine Individualisierung eines Gesichtes unabhängig vom Alter oder anderer natürlicher Veränderungen z.B. Bartwuchs. Mittels dieser Technologie wird somit ein Referenzmerkmal geschaffen, über welches eine Person jederzeit individualisiert werden kann und das daher als Anknüpfungspunkt für die Anreicherung mit weiteren Daten sehr gut geeignet ist. Sie leistet damit der Bildung von Persönlichkeitsprofilen Vorschub.

13 Auch die allgemeinen technischen Rahmenbedingungen der Erhebung, Verarbeitung

[11] Vgl. *VG Gelsenkirchen*, Beschl. v. 15.05.2012, 17 K 3382/07, Ziff. 25.
[12] Definition Biometrie, vgl. http://de.wikipedia.org/wiki/Biometrie (18.07.2012).
[13] *Roßnagel/Hornung*, Biometrische Daten in Ausweisen, DuD 2005, 69, 70.
[14] Vgl. z.B. § 28 Abs. 6 BDSG.
[15] *Gundermann/Probst*, Biometrie in: *Roßnagel* (Hrsg.), Handbuch des Datenschutzrechts, Kap. 96, Rn. 26f.

und Nutzung personenbezogener Daten führen zu einem erhöhten Gefährdungspotenzial. Betroffenen ist die Möglichkeit der Kontrolle der Weiterverwendung einmal erstellter biometrischer Templates vollständig entzogen. Die Allgegenwärtigkeit[16], Vernetzung[17] und Leistungsfähigkeit[18] informationstechnischer Systeme führt bereits für sich genommen zu einer weitgehenden Bedrohung für die Persönlichkeitsrechte der Betroffenen, wobei der bereits erwähnte Verlust der Kontrollfähigkeit der Systeme durch die Betroffenen an erster Stelle zu nennen ist. Unter diesem Eindruck müssen verantwortliche Stellen bei der Verwendung biometrischer Daten innerhalb komplexer Verarbeitungssysteme erhöhte Anforderungen an die Wahrung der Persönlichkeitsrechte der Betroffenen erfüllen. Diese können neben der Herstellung größtmöglicher Transparenz durch technische und rechtliche Dokumentation zusätzlich durch externe Auditierungen und die effektive Umsetzung der Betroffenenrechte realisiert werden.

14 Persönlichkeitsprofile stehen seit jeher unter der besonderen Beobachtung des Datenschutzes. Profile, die Ausdruck der (Teil-)Individualität einer natürlicher Personen sind, lösen regelmäßig einen Rechtfertigungsdruck hinsichtlich deren Erstellung und Verwendung auf Seiten der verantwortlichen Stelle aus.[19] Der Schutz der Betroffenen wegen der Gefährdung aufgrund der vielfachen Verwendungsmöglichkeiten und den aktuellen Bedingungen der Datenverarbeitung wird daher schon ohne Ansehen des konkreten Verarbeitungskontextes bei der Erhebung und Verarbeitung biometrischer Merkmale antizipiert. Allein das von dem biometrischen Datum ausgehende beschriebene Potenzial der Persönlichkeitsgefährdung führt zu den hohen Hürden bei der Vermessung und digitalen Verarbeitung von Körpermerkmalen.

15 ## IV. Datenschutzrechtliche Zulässigkeit der Gesichtserkennung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn ein Gesetz diese anordnet oder zulässt, oder die betroffene Person eingewilligt hat, § 4 Abs. 1 BDSG. Biometrische Templates sind personenbezogene Daten i.S.d § 3 Abs. 1 BDSG, denn sie individualisieren die auf dem Bild abgebildete Person. Gemäß § 3 Abs. 1 BDSG sind personenbezogene Daten sämtliche Angaben über die sachlichen und persönlichen Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

16 Das erstellte Template erlaubt die über das Gesicht zum Ausdruck kommende Individualität eines Menschen informationstechnisch zu verarbeiten und der weiteren Auswertung zugänglich zu machen. Die Einzigartigkeit des menschlichen Gesichts wird über das Template maschinenlesbar und ist mit der vermessenen Person unmittelbar verbunden.

17 Nicht erforderlich ist dabei, dass die abgebildete Person über das Template identifiziert wird, d.h. namentlich benennbar ist. Maßgeblich ist, dass die Information die Person von anderen Personen unterscheidbar macht.[20] Bereits die Möglichkeit, auf der Grundlage eines Referenztemplates festzustellen, ob auf zwei Bildern dieselbe Person abgebildet ist, erlaubt Rückschlüsse auf dessen persönliche und sachliche Verhältnisse und erfüllt damit den Tatbestand des § 3 Abs.1 BDSG.

[16] *BVerfG*, Urt. v. 27.2.2008, 1 BvR 370/07, Ziff. 171; http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html (18.07.2012).
[17] Fn. 16, Ziff. 175, 177.
[18] Fn. 16, Ziff. 172, 174.
[19] *BVerfG*, Urt. v. 15.12.1983, 1 BvR 209/83 u.a., NJW 1984, 412 Ziff. 171.
[20] *Buchner*, in: *Taeger/Gabel*, BDSG, § 3 Rn. 11.

S. 125

A. Anwendbarkeit deutschen Datenschutzrechts

18 In der Diskussion um die Zulässigkeit der Nutzung biometrischer Daten spielt die Diskussion um die Anwendbarkeit des deutschen Datenschutzrechts eine prominente Rolle. Vor allem für Betreiber mit Sitz außerhalb der Europäischen Union ist die Anwendbarkeit des BDSG von maßgeblicher Bedeutung. Soweit jedoch der Betreiber seinen Sitz innerhalb der Europäischen Union hat, greift das jeweils in dem Mitgliedstaat geltende nationale Datenschutzrecht.

19 Dies gilt gemäß § 1 Abs. 5 S. 2 BDSG nicht, wenn der Betreiber seinen Sitz außerhalb der Europäischen Union hat. Dann findet das BDSG auf diesen Anwendung, sofern er zur Verfolgung seines Geschäftszwecks in Deutschland personenbezogene Daten erhebt, verarbeitet oder nutzt. Die Anforderung an das Tatbestandsmerkmal der innerstaatlichen Datenerhebung i.S.d. § 1 Abs. 5 BDSG ist in Konformität mit der Europäischen Datenschutzrichtlinie auszulegen.[21] Denn § 1 Abs. 5 S. 2 BDSG setzt die Vorgaben des Art. 4 Abs. 1 lit. c) RL 95/46/EG um. Danach kommt das jeweilige Recht des Mitgliedstaates zur Anwendung, wenn die Verarbeitung der Daten von einer verantwortlichen Stelle ausgeführt wird, die nicht im Gebiet der Europäischen Union niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet dieses Mitgliedsstaats belegen sind.

20 Ob ein Betreiber in Deutschland personenbezogene Daten erhebt, verarbeitet oder nutzt, ist in normativer und technischer Hinsicht zu bestimmen.[22] Die in § 1 Abs. 5 BDSG enthaltene Normierung dient der Wahrung des bestehenden Datenschutzniveaus für die Betroffenen bei der Erhebung und Verarbeitung ihrer Daten durch Unternehmen mit Sitz außerhalb des Geltungsbereiches des deutschen bzw. europäischen Datenschutzrechts.

21 Die Rechtfertigung für die Anwendung nationaler bzw. europäischer Vorgaben im Hinblick auf die Datenverarbeitung liegt in der Bezugnahme des „Erfolgsortes“ und des Territoriums des jeweiligen Mitgliedsstaates. Art. 4 Abs. 1 lit. c) RL 46/95/EG knüpft den Bezug zwischen dem Unternehmen und dem Territorium an den Begriff der Belegenheit der Mittel. Betreiber mit Sitz außerhalb der Europäischen Union nutzen im Inland belegene Mittel, wenn sie technische Einrichtungen mit Standort im jeweiligen Mitgliedsstaat zur Datenverarbeitung verwenden oder wenn die verarbeiteten Daten in Deutschland gespeichert werden.[23] Dies trifft in der Regel zu, wenn Unterauftragnehmer, Provider o.ä. durch die verantwortliche Stelle mit technischen Dienstleistungen beauftragt werden, welche diese dann mit dem Einsatz von Hardware in dem Land erledigen. Zu derartigen Dienstleistungen gehört u.a. der Betrieb von Serverparks.

S. 126

22 Über diese recht eindeutige Nutzung technischer Mittel ist das Tatbestandsmerkmal nach Ansicht der Art. 29-Datenschutzgruppe[24] ebenfalls erfüllt, sobald z.B. Cookies oder Java Skripte, die zur Datenverarbeitung auf den Endgeräten der Betroffenen

[21] *OLG Hamburg*, Urt. v. 2. 8. 2011, 7 U 134/10, NJW-RR 2011, 1611.
[22] *Jotzo*, Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitendem Datenverkehr?, MMR 2009, 232, 236f.
[23] *Dammann,* in: *Simitis*, BDSG, 7. Aufl., 2011, Rn. 21; *LG Hamburg*, Urt. V. 07.08.2009, 324 O 650/08, Ziff. 40.
[24] Gemäß Art. 29 RL 46/95/EG ist Aufgabe der gleichnamigen Gruppe die Beratung der EU-Kommission und der Organe der EU in Datenschutzfragen. Sie setzt sich aus den Vertretern der Aufsichtsbehörden der Mitgliedsstaaten zusammen. Die von der Art-29-Gruppe veröffentlichten Arbeitspapiere haben sind von maßgeblicher Bedeutung für die Auslegung der europäischen Datenschutzrichtlinie und wirken daher bis in den nationalen Rechtsraum. Vor allem für international agierende Unternehmen bietet die Rechtauslegung der Gruppe eine Richtlinie für das einzuhaltende Datenschutzniveau im europäischen Rechtsraum.

gespeichert bzw. ausgeführt werden, durch die Betreiber zum Einsatz kommen.[25] Es fallen nicht nur Mittel im Sinn einer technischen Ausrüstung darunter. Entsprechend dem Zweck der Datenschutzrichtlinie zählen sämtliche Maßnahmen oder Medien dazu, mittels derer die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten realisiert wird.[26]

23 In der Regel greifen Betreiber sozialer Netzwerke auf Javascripte oder Cookies zurück, um zumindest den Upload der digitalen Bilder, d.h. die Erhebung der Daten, zu ermöglichen. Je nach technischer Konfiguration des gesamten Verfahrens kann es dann zu einer weiteren Datenverarbeitung auf dem Territorium des jeweiligen Staates kommen. Der Ort der Nutzung der technischen Mittel kann jedoch nicht das alleinige Anknüpfungskriterium sein. Denn die dezentrale Struktur des Internets macht es häufig vor allem für global aktive Anbieter derartiger Dienste schwer, bestimmen zu können, wo konkret die jeweiligen Daten verarbeitet werden.

24 Daher ist ein weiteres Tatbestandsmerkmal in teleologischer Auslegung des § 1 Abs. 5 BDSG zu fordern. Die Norm soll einerseits eine übermäßige Belastung der dem europäischen Datenschutzrecht unterworfenen Unternehmen verhindern, andererseits aber die Wahrung des Schutzniveaus bei Anbietern mit Sitz außerhalb der Europäischen Union sicherstellen.[27] Nur wenn durch die Unternehmen selbst die Erhebung, Verarbeitung und Nutzung von Daten der unter den Schutz der europäischen Rechtsordnung fallenden Nutzerinnen und Nutzer bezweckt wird, müssen sich diese Unternehmen den Anforderungen der europäischen Rechtsordnung unterwerfen.

S. 127

25 Unter den technischen Bedingungen des Internets würde anderenfalls das Europarecht und teilweise das nationale Datenschutzrecht einen universellen Geltungsanspruch erhalten. Denn nicht-europäische Anbieter sind nicht davor geschützt, dass Nutzerinnen und Nutzer aus Europa ihre Dienste nutzen. Vor allem dann nicht, wenn die Anbieter selbst keinen territorialen Bezug herstellen möchten, z.B. weil sich das Angebot nicht an europäische Nutzerinnen und Nutzer richtet. Den Anbietern würde bei einer rein technischen Betrachtungsweise die Beachtung der europäischen Rechtsordnung aufgedrängt werden. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten muss mit dem Willen der Anbieter im Inland erfolgen. Dies ist in der Regel der Fall, wenn Betreiber sozialer Netzwerke ihr Angebot den Nutzerinnen und Nutzer des jeweiligen Landes bewusst zur Verfügung stellen. Ein maßgebliches Indiz dafür ist die Nutzung entsprechender Top-Level-Domains (TLD) oder die Abfassung des Angebots in der jeweiligen Landessprache.

26 **B. Zulässigkeit aufgrund gesetzlicher Rechtfertigungstatbestände**

Die Zurverfügungstellung einer Uploadfunktionalität ist ein Erheben, § 3 Abs. 3 BDSG, die Auswertung von hochgeladen Fotos und die Erstellung von biometrischen Templates eine Verarbeitung personenbezogener Daten gemäß § 3 Abs. 4 BDSG. Die Rechtfertigungsanforderung des § 4 Abs. 1 BDSG muss daher durch den jeweiligen Betreiber erfüllt werden. Eine derartige Rechtfertigungspflicht entspricht den Vorgaben der Europäischen Datenschutzrichtlinie, Art. 7 RL 95/46/EG.

27 Das Bundesdatenschutzgesetz, welches gemäß § 1 Abs. 2 BDSG auf die Bundesbehörden und die Wirtschaft Anwendung findet, sieht im 3. Abschnitt eine Reihe von gesetzlichen Zulässigkeitstatbeständen vor.

28 Für Betreiber sozialer Netzwerke ist dabei § 28 BDSG von maßgeblicher Bedeutung. Denn die genutzten digitalen Bilder sind als Inhaltsdaten zu qualifizieren und

[25] *Art. 29-Datenschutzgruppe*, Stellungnahme 8/2010 zum anwendbaren Recht v. 16. Dezember 2010, WP 179, 0836-02/10/DE, S. 26.
[26] Fn. 24, S. 25.
[27] *Gola/Schomerus*, BDSG, 10. Aufl. 2011, § 1 Rn. 27f.

unterfallen damit dem Rechtsregime des BDSG.[28] Das BDSG trennt zwischen der Verwendung personenbezogener Daten zu eigenen, § 28 BDSG, und fremden, § 29 BDSG, Geschäftszwecken.[29] Soweit Betreiber sozialer Netzwerke die erstellten biometrischen Profile zur Verbesserung oder z.B. Bewerbung ihres eigenen Angebotes verwenden, greifen die Rechtfertigungsgründe des § 28 BDSG ein.

S. 128

29 **1. Rechtfertigung aufgrund entsprechenden Vertragsabschlusses, § 28 Abs. 1 Nr. 1 BDSG**

Soweit zwischen den Betreibern sozialer Netzwerke und den Nutzerinnen und Nutzern ein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis bei der Nutzung entsteht, kann die Erhebung und Verarbeitung der digitalen Bilder zulässig sein, wenn dies für die Begründung, Durchführung oder Beendigung ebendieses Rechtsverhältnisses erforderlich ist. Das Merkmal der Erforderlichkeit begrenzt den Umfang der Datenerhebung für die Betreiber dahingehend, dass der Zweck des Rechtsgeschäfts nur erfüllt werden kann, wenn die in Frage stehenden Verarbeitungsprozesse in der vorgesehenen Art und dem Umfang durchgeführt werden.[30] Sobald das Ziel des Rechtsgeschäfts anderweitig, d.h. ohne die rechtfertigungsbedürftige Datenverarbeitung erreicht werden kann, wird das Merkmal der Erforderlichkeit nicht erfüllt und die Verwendung der Daten läßt sich nicht auf diesen Rechtfertigungsgrund stützen.

30 Maßgeblich ist daher der Inhalt des geschlossenen Nutzungsvertrags. In der Regel wird jedoch weder für die Begründung noch für die Nutzung oder für die Beendigung der Nutzung eines sozialen Netzwerkes das Verfahren der Gesichtserkennung erforderlich sein. Denn Nutzerinnen und Nutzer können sich ohne die Erfassung biometrischer Merkmale in Netzwerken mit einander verbinden. Das Markieren von Bildern erfordert keine biometrische Erfassung der hochgeladenen Informationen. Für die Erfüllung des Nutzungsverhältnisses ist die Gesichtserkennung i.d.R. kein unabdingbarer Verarbeitungsprozess. Nur in den Fällen, in denen die Nutzung des Dienstes ausschließlich darin besteht, sich maßgeblich über Bilder mit anderen Nutzerinnen und Nutzern zu vernetzen, kann eine andere rechtliche Bewertung vertretbar sein.

31 **2. Rechtfertigung durch berechtigten Interesses, § 28 Abs. 1 Nr. 2 und Abs. 2 Nr. 2a) BDSG**

In Betracht käme, dass sich Betreiber sozialer Netzwerke auf das berechtigte Interesse gemäß § 28 Abs. 1 Nr. 2 BDSG und § 28 Abs. 2 Nr. 2 a) BDSG berufen. Danach ist die Verarbeitung personenbezogener Daten zur Verfolgung berechtigter Interessen der verantwortlichen Stelle oder der berechtigten Interessen eines Dritten zulässig, soweit die Verarbeitung zur Verfolgung des Zwecks erforderlich ist und kein Grund zu der Annahme besteht, dass die schutzwürdigen Interessen der Betroffenen der Verarbeitung entgegenstehen. Unter dem Begriff des berechtigten Interesses werden alle, auf eine konkrete Verarbeitung gerichteten, von der Rechtsordnung gebilligten Geschäftsinteressen verstanden.[31]

S. 129

32 Betreibern sozialer Netzwerke kann nicht abgesprochen werden, die Nutzung ihrer Dienste so attraktiv, komfortabel und innovativ wie möglich auszugestalten. Denn dies kann gegenüber den Konkurrenten ein maßgeblicher Marktvorteil sein. Zu diesem Zweck können sie sich Verfahren wie der Gesichtserkennung bedienen und darüber ein

[28] Str. vgl. *Karg/Fahl*, Datenschutz in sozialen Netzwerken, K&R 2011, S. 453, 458.
[29] *Taeger*, in *ders./Gabel*, BDSG, § 28, Rn. 15.
[30] *Ambs* in: *Erbs/Kohlhaas,* Strafrechtliche Nebengesetze, 188. Erglfg. 2012, BDSG, § 14 Rn. 5; *Gola/Schomerus,* BDSG 10. Aufl. 2010, § 28 Rn. 14f.
[31] *Taeger* in: *ders/Gabel*, BDSG, § 28 Rn. 55f.

berechtigtes Interesse an der Nutzung digitaler Bilder haben.

33 Dem stehen jedoch die schutzwürdigen Interessen der Betroffenen entgegen. Wie bereits im Rahmen der Risikoanalyse dargelegt, stellen die erstellten Templates eine digitale Signatur des Gesichts der betroffenen Personen dar. Je öfter Bilder einer Nutzerin oder eines Nutzers erhoben und abgeglichen werden, desto detaillierter wird das in der Datenbank gespeicherte Referenztemplate. Gesichter sind Ausdruck der Individualität des Einzelnen. Mit der fortgesetzten qualitativen Verbesserung der Individualisierung von Personen mittels des Aufbaus biometrischer Datenbanken werden die Templates sukzessive zu digitalen Gesichtsabdrücken. Die Erfassung dieser Individualität stellt einen direkten Bezug zu der in Art. 1 Abs. 1 GG geschützten Menschenwürde her. Verfassungsrechtlich ist der Eingriff in die Menschenwürde ohnehin nicht rechtfertigbar.[32] Neben dieser potenziellen Verletzung verfassungsrechtlich geschützter Güter können sich weitere zahlreiche Gefährdungen für das Recht auf informationelle Selbstbestimmung entwickeln (s.o.). So kann die verfassungsrechtlich geschützte Anonymität in der Öffentlichkeit[33] durch die Fortentwicklung dieser Technologie bedroht werden. Der Schutz des Grundrechts auf informationelle Selbstbestimmung der Betroffenen wird daher in der Regel die berechtigten Interessen der Betreiber an der Verarbeitung von Bilddaten zum Zweck der biometrischen Erfassung und Speicherung überwiegen.

34 Aus diesen Gründen sind die derzeit geltenden gesetzlichen Erlaubnistatbestände nicht geeignet, Verfahren der biometrischen Gesichtserkennung zu legitimieren.

35 C. Einwilligungserfordernis gemäß § 4a BDSG

Die Verarbeitung der Bilddaten zum Zweck der biometrischen Vermessung und Erstellung von Templates und die Speicherung dieser Daten ist nur mit einer den Anforderungen des § 4a BDSG entsprechenden Einwilligung rechtfertigbar. Gemäß § 4 a BDSG müssen Einwilligungen informiert, bewusst und freiwillig erteilt werden.[34] Konkludentes Verhalten oder ein Unterlassen einer Handlung erfüllt den Tatbestand dieser Vorschrift nicht. Daher ist der immer wieder zu hörende Verweis auf die Freiwilligkeit der Nutzung sozialer Netzwerke rechtlich unbeachtlich.

36 Nutzerinnen und Nutzer müssen in Kenntnis der Tragweite ihrer Entscheidung die Einwilligung erteilen und diese ohne äußeren Zwang treffen. Verfahren, die Widerspruchslösungen (opt-out) als Rechtfertigung anbieten,[35] entsprechen nicht den Vorgaben des § 4a BDSG. Rückgriffe auf Nutzungsbedingungen oder Datenschutzerklärungen können den Einsatz der Gesichtserkennung ebenfalls nicht legitimieren. Denn in den genannten Varianten werden die Nutzerinnen und Nutzer nicht vor dem Beginn der Datenverarbeitung aufgefordert, eine Entscheidung zu treffen. Der Eingriff in die Rechte der Betroffenen erfolgt, ohne dass diese auf den Beginn des Verarbeitungsprozesses Einfluss nehmen können.

37 D. Zulässigkeit auf der Grundlage der EU-Datenschutzrichtlinie 95/46/EG

Die geäußerte Forderung nach der Einholung einer Einwilligung der Betroffenen vor der Erhebung und Verarbeitung digitaler Bildinformationen zum Zweck der Gesichtserkennung entspricht den Forderungen der Art. 29-Datenschutzgruppe. § 4a BDSG ist in Umsetzung des Art. 7 lit. a RL 95/46/EG erlassen worden. Nach dem Wortlaut der Richtlinie darf die Verarbeitung personenbezogener Daten lediglich erfolgen, wenn die betroffene Person „ohne jeden Zweifel ihre Einwilligung gegeben“

[32] *Jarass/Pieroth*, GG, 10. Aufl. 2009, Art. 1 Rn. 16.
[33] *BVerfG*, 1 BvR 2368/06 vom 23.2.2007, Absatz-Nr. 39, http://www.bverfg.de/entscheidungen/rk20070223_1bvr236806.html.
[34] *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 4a Rn. 6, 10.
[35] Siehe beispielhaft Facebook unter https://www.facebook.com/help/?faq=187272841323203 (18.07.2012).

hat. In einem Arbeitspapier zur Auslegung des Art. 7 lit. a RL 95/46/EG hat die Art. 29-Datenschutzgruppe klargestellt, dass Datenverarbeiter durch diese Vorgaben zur Einführung robuster Prozeduren verpflichtet werden, die das Vorliegen einer wirksamen Einwilligung sicherstellen. Voreinstellungen in sozialen Netzwerken, die eine Einwilligung fingieren sollen entsprechen diesen Anforderungen nicht. Das Nichtändern solcher Einstellungen hat keinen bzw. keinen eindeutigen Erklärungswert.[36]

S. 131

38 Die Forderung nach einer expliziten, vorherigen Einwilligung der Betroffenen entspricht darüber hinaus dem europäischen Standard. In einer weiteren, konkret auf das Verfahren der Gesichtserkennung abzielenden Auslegungshilfe stellte die Art. 29-Datenschutzgruppe fest, dass die Erstellung dauerhafter Referenztemplates nur mit der vorherigen ausdrücklichen Einwilligung der Betroffenen zulässig sei. Lediglich die Erstellung temporärer Templates, mittels derer das Vorliegen einer Einwilligung geprüft wird und die nach diesem Prozess entweder gelöscht oder zum Referenztemplate hinzugespeichert werden, soll ohne Einwilligung zulässig sein.[37] D.h. die primäre Erstellung des biometrischen Templates wäre ohne Einwilligung zulässig. Voraussetzung ist jedoch, dass dieses Template lediglich dazu genutzt wird festzustellen, ob ein Referenztemplate existiert, d.h. die Person in die Erstellung biometrischer Templates eingewilligt hat und im Falle des Nichtvorliegens der Einwilligung das Template unverzüglich gelöscht wird:

39 *Because of the particular risks involved with biometric data, this will therefore require the informed consent of the individual prior to commencing the processing of digital images for facial recognition. However, in some cases, the data controller may temporarily need to perform some facial recognition processing steps precisely for the purpose of assessing whether a user has provided consent or not as a legal basis for the processing. This initial processing (i.e. image acquisition, face detection, comparison, etc) may in that case have a separate legal basis, notably the legitimate interest of the data controller to comply with data protection rules. Data processed during these stages should only be used for the strictly limited purpose to verify the user's consent and should therefore be deleted immediately after.*[38]

40 Der Eingriff in die Rechte der Betroffenen, die nicht in die Nutzung ihrer Daten eingewilligt haben oder dies nicht konnten, z.B. weil sie nicht Mitglied des jeweiligen Netzwerkes sind, wird für eine juristische Sekunde hingenommen. Vorrausetzung dafür ist jedoch, dass der Eingriff über dieses Maß nicht hinausgeht. Eine weitere Nutzung der erstellten Templates wäre unzulässig.

S. 132

41 **V. Zulässigkeit der Speicherung erstellter Templates von Nichtnutzern**

Diese rechtliche Bewertung dürfte mit der Rechtsprechung des Bundesverfassungsgerichtes[39] in ähnlich gelagerten Fällen im Einklang stehen. Und es könnte eine Antwort auf die Frage sein, wie Netzwerkbetreiber ihrer Verpflichtung zur Einholung einer Einwilligung vor der Erhebung von Daten von Nichtnutzerinnen und Nichtnutzern nachkommen können.

42 In der zitierten Entscheidung zur Kennzeichenerfassung, hatte das Bundesverfassungsgericht über die verfassungsrechtliche Zulässigkeit der automatisierten Erhebung von Kfz-Kennzeichen zu befinden. Die Kennzeichen wurden

[36] Art. 29-Datenschutzgruppe, Opinion 15/2011 on the definition of consent, Working Paper 187, 01197/11/EN, S. 21, 24.
[37] Art. 29-Datenschutzgruppe, Opinion 02/2012 on facial recognition in online and mobile services, Working Paper 192, 00727/12/EN, S. 5.
[38] S. Fn. 36.
[39] BVerfG, Urt. v. 11.3.2008, 1 BvR 2074/05, 1. Leitsatz und Ziff. 62ff., http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html (18.07.2012).

durch Erfassungsgeräte am Straßenrand unterschiedslos automatisiert erhoben. Innerhalb kürzester Zeit wurden die erfassten Kennzeichen dann mit einer internen Datenbank gesuchter Kennzeichen abgeglichen. Nur wenn bei dem Abgleich eine Übereinstimmung zwischen der erfassten Nummer und einem gespeicherten Kennzeichen festgestellt wurde, erfolgte eine weitere Verarbeitung der Information. Fehlte eine derartige Übereinstimmung, wurde die Nummer unverzüglich und restlos gelöscht.

43 Das Bundesverfassungsgericht stellt in der Entscheidung fest, dass der Schutzumfang des Rechts auf informationelle Selbstbestimmung auch die durch eine Datenverarbeitung verursachte und einer konkrete Rechtsgüterbeeinträchtigung vorgelagerte Gefährdungslage erfasst.[40] Andererseits sah das Bundesverfassungsgericht keinen Eingriff in der Erhebung in das Recht auf informationelle Selbstbestimmung soweit, „Daten unmittelbar nach der Erfassung technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden."

44 Eine datenschutzrechtliche Bewertung der Erstellung biometrischer Templates von Nichtnutzern und die strenge Umsetzung des Einwilligungserfordernisses führt zu einem Dilemma: Netzwerkbetreiber können sich kaum davor schützen, dass auch Bilder von Personen durch die Nutzerinnen und Nutzer eingestellt werden, auf denen Personen abgebildet sind, die nicht Mitglied des Dienstes sind. Bei einer konsequenten Anwendung des Verbots mit Erlaubnisvorbehaltes i.S.d. § 4 Abs. 1 BDSG, müsste der Betreiber vor der Erstellung des Templates die abgebildete Person um die Einwilligung bitten. Eine Nutzung der Bilddaten wäre rechtlich nur zulässig, wenn bereits vorher entweder die Nutzerinnen und Nutzer zusätzlich zu den eingestellten Fotos auch weitere Kontaktdaten über die abgebildeten Nichtnutzerinnen und Nichtnutzern dem Netzwerkbetreiber zur Verfügung stellen oder sich dieser derartige Informationen anderweitig beschafft.

S. 133

45 Selbst wenn Einwände zur Praktikabilität einer derartigen Forderung zur Seite geschoben würden, ist deutlich, dass damit der Betreiber eine größere Informationsmenge über die Nichtnutzerinnen und Nichtnutzer erhält, als dies bei einer bloßen Auswertung der Bilddaten der Fall sein würde. Ansichten, die sich der normativen Kraft des Faktischen standhaft widersetzen, würden die Unzulässigkeit des Einsatzes derartiger Technologien innerhalb sozialer Netzwerke konstatieren.

46 Unter Anwendung der in der erwähnten Rechtsprechung vorgegebenen Richtlinien für die Bestimmung des Eingriffs in das Recht auf informationelle Selbstbestimmung und Rückgriff auf die Auffassung der Art-29-Gruppe ist jedoch ein Lösungsweg skizzierbar.

47 Zur Rechtfertigung der Erstellung biometrischer Templates von Nichtnutzerinnen und Nichtnutzern durch Betreiber von Telemediendiensten zur Ausgestaltung ihres Dienstes könnte § 28 Abs. 1 Nr. 2 BDSG herangezogen werden. Dazu müsste jedoch der Betreiber sicherstellen, dass

48 • die Templates lediglich zur Feststellung genutzt werden, ob die abgebildete Person Mitglied des Netzwerkes ist und eine Einwilligung zur dauerhaften Speicherung des Templates erteilt hat,

49 • nach dieser Feststellung unverzüglich, d.h. ohne weitere technische Zwischenschritte das Template gelöscht wird,

50 • sichergestellt ist, dass auch darüber hinausgehende Auswertungen nicht erfolgen, d.h. die Feststellung der Identität der abgebildeten Person nicht anderweitig realisiert wird und

[40] Fn. 39, Ziff. 64.

51 • Betreiber die Einhaltung der genannten Bedingungen nachvollziehbar dokumentieren und die Prüffähigkeit des Verfahrens[41] sicherstellen.

52 Nur unter den genannten Bedingungen ist der Schutz der Persönlichkeitsrechte derjenigen, die keinen Kontakt zu den Betreibern sozialer Netzwerke haben, ansatzweise herstellbar. Es ist die Verpflichtung der Betreiber sicherzustellen, dass ihre Angebote nicht zu Kollateralschäden bei denjenigen führen, die die Dienste entweder nicht nutzen wollen oder nicht nutzen können.

S. 134

53 ## VI. Fazit

Verfahren der Gesichtserkennung sind ohne ausdrückliche Einwilligung der Betroffenen in der Regel datenschutzrechtlich unzulässig. Aufgebaute Datenbestände, die weder durch einen gesetzlichen Rechtfertigungstatbestand noch durch die Einwilligung der Betroffenen legitimiert sind, müssen gemäß § 35 Abs. 2 Nr. 1 BDSG gelöscht werden. Die gesetzlichen Regelungen sehen eine nachträgliche Legitimierung nicht vor.

54 Wie in anderen Bereichen der modernen Kommunikations- und Informationstechnologie muss bei diesen Verfahren die Unzulänglichkeit der gesetzlichen Regeln beklagt werden. Die Bedrohung des Verlustes der Anonymität in der Öffentlichkeit hat Auswirkungen auf unser demokratisches Gemeinwesen. Der Gesetzgeber ist daher gefordert, Rahmen und Umfang der Zulässigkeit des Einsatzes derartiger Technologien abzustecken. Dabei ist das Grundprinzip, dass jede und jeder selbst über die Verwendung seiner Daten bestimmen kann und muss, zu achten.

Zitierempfehlung: Moritz Karg, HFR 2012, S. 120 ff.

[41] *Unabhängiges Landeszentrum für Datenschutz*, 29. Tätigkeitsbericht, 2007, Kap. 6.1, https://www.datenschutzzentrum.de/material/tb/tb29/kap06.htm#61 (18.07.2012).