Der Elektronische Rechtsverkehr 48

Hanna Hoffmann

Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO

Eine Gefahr für die Autonomie (?)

Nomos

Der Elektronische Rechtsverkehr

Herausgegeben von
Prof. Dr. Alexander Roßnagel und
Prof. Dr. Gerrit Hornung, LL.M.
in Zusammenarbeit mit
dem TeleTrusT Deutschland e.V.

Band 48

Hanna Hoffmann

Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO

Eine Gefahr für die Autonomie (?)

Nomos

Onlineversion
Nomos eLibrary

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliographische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Münster (Westf.), Univ., Diss. der Rechtswissenschaftlichen Fakultät, 2022

ISBN 978-3-7560-0065-4 (Print)
ISBN 978-3-7489-1474-7 (ePDF)

D6

1. Auflage 2023

Meiner Familie

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2022 von der Rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität Münster als Dissertation angenommen. Sie entstand während meiner Tätigkeit als wissenschaftliche Mitarbeiterin der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM). Rechtsprechung und Literatur wurden bis Mai 2022 berücksichtigt.

Außerordentlicher Dank gebührt meinem Doktorvater Herrn Prof. Dr. Thomas Hoeren, der diese Arbeit nicht nur angeregt, sondern ihre Fertigstellung nach Kräften gefördert hat. Dabei ließ er mir einerseits vertrauensvoll großen wissenschaftlichen Freiraum, stand mir andererseits aber bei Diskussionsbedarf stets prompt und engagiert zur Seite.

Herrn Prof. Dr. Kai von Lewinski danke ich herzlich für die äußerst rasche Erstellung des Zweitgutachtens. Herrn Prof. Dr. Alexander Roßnagel und Prof. Dr. Gerrit Hornung danke ich für die Aufnahme in ihre Schriftenreihe.

Für die schöne Zeit und vielen freundschaftlichen wie fachlichen Gespräche am ITM bedanke ich mich bei allen Kolleginnen und Kollegen, ganz besonders bei Dr. Julia Werner, Dr. Verena Vogt, Nicolas John, Dr. Johannes Kevekordes und Lukas Willeke. Für den wertvollen Austausch über das maschinelle Lernen gilt mein Dank ferner Thomas Buddenkotte. Besonders gedankt sei auch Dr. Andreas Bruns für die Gespräche über die ethischen Grundlagen der Autonomie. Schließlich möchte ich Viviana Kämper, Charlotte Presto, Nicolas John und Hendrik Rumler herzlich danken, die sich mit großem Engagement der mühevollen Aufgabe des Korrekturlesens angenommen haben.

Meinen Eltern Thomas und Ulrike, meinen Geschwistern Lukas und Marie sowie meiner Großmutter Momi möchte ich dafür danken, dass sie meinen bisherigen Lebensweg mit uneingeschränktem Zuspruch begleitet haben und mir ohne Zögern jegliche erdenkliche Unterstützung haben zukommen lassen. Ihnen ist diese Arbeit in Liebe und Dankbarkeit gewidmet.

Ohne den Rückhalt meines Verlobten Hendrik wäre das Projekt „Dissertation“ schließlich nicht möglich gewesen. Hierfür bedanke ich mich von Herzen.

Münster, im Dezember 2022 Hanna Hoffmann

Inhaltsverzeichnis

Abkürzungsverzeichnis

Artif. Intell. Rev.	Artificial Intelligence Review
Berkeley Technol. Law J.	Berkeley Technology Law Journal
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
bidt	Bayerische Forschungsinstitut für Digitale Transformation
Big Data Soc.	Big Data and Society
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
Boston Univ. Law Rev.	Boston University Law Review
Columbia Bus. Law Rev.	Columbia Business Law Review
Commun. ACM	Communications of the ACM
Comput. Vis. Image Underst.	Computer Vision and Image Understanding
CVF	Computer Vision Foundation
CNIL	Commission Nationale de l'Informatique et des Libertés
DSB	Datenschutzbehörde Österreich
DSRL	Europäische Datenschutz-Richtlinie 95/46/EG
EDPB	Europäischer Datenschutzausschuss
EDPS	Europäischer Datenschutzbeauftragter
EFF	Electronic Frontier Foundation
EDÖB	Schweizerische Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte
et al.	et alii
Ethics Inf. Technol.	Ethics and Information Technology
ECCV	European Conference on Computer Vision
ErwG	Erwägungsgrund

EWSA	Europäischer Wirtschafts- und Sozialausschuss
F.A.Z.	Frankfurter Allgemeine Zeitung
Forensic Sci. Int.	Forensic Science International
FRA	Agentur der Europäischen Union für Grundrechte
Geo. L. Tech. Rev.	Georgetown Law Technology Review
GPDP	Garante per la protezione dei dati personali (Italienische Datenschutzbehörde)
Harv. Law Rev.	Harvard Law Review
HDBI	Hessische Datenschutzbeauftragte
HmbBfDI	Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Hum. Factors	Human Factors
i.E.	im Ergebnis
IMY	Integritetsskyddsmyndigheten (Schwedische Datenschutzbehörde)
ICLR	International Conference on Learning Representations
ICO	Information Commissioner's Office (Datenschutzbeauftragter des Vereinigten Königreichs)
IDPL	International Data Privacy Law
IEEE	Institute of Electrical and Electronics Engineers
Int. J. Comput. Vis.	International Journal of Computer Vision
Internet Policy Rev.	Internet Policy Review
JI-RL	Europäische Justiz-und-Inneres-Datenschutz-Richtlinie (EU) 2016/680
JMLR	Journal of Machine Learning Research
J. Manage. Inf. Syst.	Journal of Management Information Systems
J. Philos.	Journal of Philosophy
JRE	Jahrbuch für Recht und Ethik

J. Technol. Law Policy	Journal of Law, Technology & Policy
Law Innov. Technol.	Law, Innovation and Technology
LfDI BW	Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg
l. Sp.	linke Spalte
LZ	Lebensmittelzeitung
Mach. Learn.	Machine Learning (Journal)
Midwest Stud. Philos.	Midwest Studies in Philosophy
Minn. L. Rev.	Minnesota Law Review
Nat. Commun.	Nature Communications
Neural Comput.	Neural Computation
NIST	National Institute of Standards and Technology
Nlets	International Public Safety and Justice Network
OAIC	Office of the Australian Information Commissioner
OPC	Office of the Privacy Commissioner of Canada
Philos.' Impr.	Philosophers' Imprint
Philos. Technol.	Philosophy & Technology
PNAS	Proceedings of the National Academy of Sciences
PMLR	Proceedings of Machine Learning Research
Psychol. Sci. Public Interest	Psychological Science in the Public Interest
Psychon. Bull. Rev.	Psychonomic Bulletin & Review
Procedia Soc. Behav. Sci.	Procedia - Social and Behavioral Sciences
r. Sp.	rechte Spalte
RefE	Referentenentwurf
Univ. Pa. Law Rev.	University of Pennsylvania Law Review
taz	Die Tageszeitung
Theor. Inq. Law	Theoretical Inquiries in Law
Univ. Chic. Leg. Forum	University of Chicago Legal Forum

Wash. Law Rev.	Washington Law Review
Yale Law J.	Yale Law Journal

Im Übrigen folgen die Abkürzungen dem Abkürzungsverzeichnis der Rechtssprache, begr. von *Kirchner, Hildebert*, bearb. von *Böttcher, Eike*, 10. Aufl. Berlin 2021.

Einleitung

A. Problemaufriss

Bereits seit mehreren Jahren ist ein zunehmendes Interesse an der Erfassung biometrischer Gesichtsdaten wahrnehmbar. Mittlerweile wird die Technologie in beinahe 100 Staaten verwendet.[1] Die vorliegende Arbeit soll der Frage nachgehen, woher dieses Interesse rührt und ob durch den Einsatz von Gesichtserkennungssystemen eine Gefahr für das autonome Leben besteht.

Spätestens seitdem die New York Times im Januar 2020 über die Gesichtserkennungssoftware des Unternehmens Clearview AI berichtet hat, ist eine breite Debatte über den Einsatz von biometrischer Gesichtserkennungstechnik entfacht.[2] Die Befürworter[3] der Technik berufen sich auf eine Stärkung der Sicherheit im öffentlichen Raum und relativieren die Tatsache, dass für nichtstaatliche Stellen häufig in erster Linie wirtschaftliche Interessen im Vordergrund stehen.[4] Die Gegner von Gesichtserkennungstechnik weisen auf die Gefahren durch missbräuchliche Verwendung und eine mögliche individuelle, aber auch gesamtgesellschaftliche Veränderung, die durch das Gefühl der ständigen Überwachung angetrieben werden kann, hin.[5]

Der ehemalige *HmbBfDI Johannes Casper* hat in seinem 29. Tätigkeitsbericht die automatisierte Gesichtserkennung als eine der größten Gefahren für die Privatsphäre bezeichnet.[6] Biometrische Gesichtserkennungsverfahren unterscheiden sich erheblich von den bisher bekannten Techniken:[7]

---

1 Siehe dazu die Übersicht des Unternehmens Surfshark, The Facial Recognition World Map, abrufbar unter: https://surfshark.com/facial-recognition-map.

2 *Hill*, The Secretive Company That Might End Privacy as We Know It, New York Times v. 18.1.2020, abrufbar unter: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

3 Aufgrund der besseren Lesbarkeit wird im Text das generische Maskulinum verwendet. Gemeint sind jedoch immer alle Geschlechter.

4 Siehe Teil 1, D.

5 Siehe Teil 4.

6 *HmbBfDI*, 29. Tätigkeitsbericht Datenschutz 2020, S. 16.

7 Ausführlich zur Bedeutung des menschlichen Gesichts im Zusammenhang mit Gesichtserkennungstechnik siehe Teil 1.

Die Gesichtsstruktur eines jeden Menschen ist einzigartig und kann nicht verändert werden. Anders als die Fingerkuppenhaut zeigt man sein Gesicht jedes Mal, wenn man den öffentlichen Raum betritt. Zudem gibt es im Internet, insbesondere in den sozialen Netzwerken, bereits eine große Menge an frei zugänglichen Gesichtsaufnahmen, die bestimmten Personen zugeordnet werden können. Schließlich kann die Technik unbemerkt und aus der Ferne eingesetzt werden.

Einer Gefahr kommt ein anderes Gewicht zu, wenn es Gesetze gibt, die die Betroffenen effektiv vor den Beeinträchtigungen schützen. So verwundert es nicht, dass es seit Jahren Forderungen nach einer Regulierung der Gesichtserkennungstechnik gibt. Bereits im Jahr 2011 hat der damalige CEO von Google *Eric Schmidt* auf der Google „Big Tent"-Konferenz die Auswirkungen des Einsatzes von Gesichtserkennungssoftware als zu gruselig (engl. „too creepy") bezeichnet.[8] Im Juni 2018 forderte der Präsident von Microsoft *Brad Smith* den Einsatz von Gesichtserkennungssoftware zu regulieren.[9] Amazon und IBM schlossen sich dieser Forderung an und veröffentlichten Leitfäden, die bei der Entwicklung eines Gesetzesrahmens als Hilfe dienen sollen.[10]

Die Europäische Kommission hat im April 2021 den weltweit ersten Regulierungsentwurf für Künstliche Intelligenz, der auch für Gesichtserkennungstechnik konkrete Vorgaben vorsieht, vorgelegt. Da ein Abschluss des Gesetzgebungsprozesses noch nicht in Sicht ist, steht die Datenschutz-Grundverordnung derzeit im Mittelpunkt der rechtlichen Beurteilung.

Trotz des großen Interesses an Gesichtserkennung sei darauf hingewiesen, dass einzelne Staaten und Städte den Einsatz der Technologie be-

---

8 *Bradshaw*, Google warns against 'foolish' legislation, Financial Times v. 18.5.2011, abrufbar unter: https://www.ft.com/content/fe240804-816d-11e0-9c83-00144feabdc0; *Warman*, Google warns against facial recognition database, The Telegraph v. 18.5.2011, abrufbar unter: //www.telegraph.co.uk/technology/google/8522574/Google-warns-against-facial-recognition-database.h//www.telegraph.co.uk/technology/google/8522574/Google-warns-against-facial-recognition-database.html; *o.V.*, 'Too creepy even for Google': Search engine boss warns governments against facial recognition technology, Daily Mail v. 20.5.2011, abrufbar unter: https://www.dailymail.co.uk/sciencetech/article-1388855/Google-CEO-Eric-Schmidt-warns-governments-facial-recognition-technology.html.

9 *Smith*, Facial recognition technology: The need for public regulation and corporate responsibility, Microsoft Blogs v. 13.7.2018, abrufbar unter: https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility.

10 https://blog.aboutamazon.com/policy/some-thoughts-on-facial-recognition-legislation; https://www.ibm.com/blogs/policy/facial-recognition-export-controls.

reits verbieten und Pilotprojekte wieder eingestellt haben. Eine geplante Einführung einer Ermächtigungsgrundlage ins deutsche BPolG zur staatlichen Überwachung von Flughäfen und Bahnhöfen ist gescheitert.[11] In Großbritannien wurde nach lauter Kritik ein kontaktloses Bezahlsystem in Schulkantinen, das Gesichtserkennungstechnik nutzte, wieder eingestellt.[12] In Belgien musste ein Pilotprojekt, das Gesichtserkennungstechnik zur Überwachung eines Flughafens nutzte, infolge einer Gesetzesänderung vorzeitig beendet werden.[13] Mehrere Städte in den USA haben staatlichen und teilweise auch nichtstaatlichen Stellen den Einsatz von Gesichtserkennungstechnik ausdrücklich untersagt.[14]

B. Untersuchungsgegenstand und Methode

Gegenstand der Untersuchung sollen zwei Kernfragen sein: Zunächst soll der Frage nachgegangen werden, ob der nichtstaatliche Einsatz von biometrischen Gesichtserkennungssystemen in das autonome Leben eingreift. Seit geraumer Zeit wird davor gewarnt, dass Informationstechnologien die Bevölkerung zunehmend abhängig von dem Willen derjenigen machen, die diese Systeme einsetzen, indem umfangreiche Daten mit Personenbe-

---

11 *o.V.*, Bundespolizeigesetz. Seehofer verzichtet auf Software zur Gesichtserkennung, Spiegel v. 24.1.2020, abrufbar unter: https://www.spiegel.de/politik/deutschland/bundespolizeigesetz-seehofer-verzichtet-auf-software-zur-gesichtserkennung-a-c207b3c8-eb1a-48e9-80ce-2642b420bd55.

12 *o.V.*, Schools pause facial recognition lunch plans, BBC v. 25.10.2021, abrufbar unter: https://www.bbc.com/news/technology-59037346.

13 Vgl. Belgisches Staatsblatt v. 16.4.2018, S. 33708, Art. 78, der die Einführung des Art. 8/1 in das „Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance" bestimmt. Überwachungskameras, die mit Referenzdatenbanken verbunden sind, werden demnach verboten, sofern sie nicht ausschließlich der automatischen Kontrolle von Kfz-Kennzeichen dienen.

14 Siehe bspw. in Kalifornien, California's Assembly Bill No 1215, Sec. 2(b) ("A law enforcement agency or law enforcement officer shall not install, activate, or use any biometric surveillance system in connection with an officer camera or data collected by an officer camera"); siehe in Portland, Portland's Ordinance 34.10.030 ("a Private Entity shall not use Face Recognition Technologies in Places of Public Accommodation within the boundaries of the City of Portland"), wobei Ausnahmen von dem Verbot in 34.10.040 vorgesehen sind; zum Verbot in Baltimore siehe *Rudl*, Portland verbietet Videoüberwachung mit Gesichtserkennung, Netzpolitik v. 10.9.2020, abrufbar unter: https://netzpolitik.org/2020/privatsphaere-portland-verbietet-videoueberwachung-mit-gesichtserkennung.

zug erfasst werden und das Verhalten analysiert wird.[15] Es wird befürchtet, dass die Verwendung von personenbezogenen Informationen, mit der Absicht die individuelle Entscheidungsfindung zu beeinflussen, nicht bloß die jeweiligen Interessen, sondern vielmehr die Autonomie beeinflusst.[16] Diese These soll aus ethischer Perspektive heraus erörtert werden und es soll der Frage nachgegangen werden, ob und inwiefern sich die Überlegungen auf den Einsatz von Gesichtserkennungssystemen übertragen lassen. In einem zweiten Schritt soll mittels einer ethischen Analyse des Rechts untersucht werden, inwiefern die individuelle Autonomie durch das geltende Recht vor Bedrohungen durch den Einsatz von Gesichtserkennungssystemen geschützt wird.

Die Arbeit nimmt den nichtstaatlichen Einsatz von Gesichtserkennungssystemen in den Blick. Nichtstaatlich sind diejenigen Stellen, hinter denen kein Hoheitsträger steht.

C. Gang der Untersuchung

Die Arbeit gliedert sich entsprechend der soeben aufgeworfenen Problemkreise in sechs Teile. Der erste Teil wendet sich der besonderen Bedeutung des menschlichen Gesichts zu. Darauf folgt der zweite Teil, in dem die technische Funktionsweise von Gesichtserkennungssystemen erläutert wird. Auf eine Darstellung der wesentlichen Grundlagen des maschinellen Lernens als Basistechnologie der Gesichtserkennung, folgt eine Erläuterung der Funktionsweise der „einfachen" Gesichtserkennungstechnik und deren Implementierung in unterschiedliche Verwendungsmöglichkeiten. Der zweite Teil schließt mit einem Einblick in die informationstechnische Sicherheit solcher Systeme und potentiellen Gefahren durch weitere Einsatzmöglichkeiten. Im dritten Teil werden die ethische Analyse des Rechts als Bewertungsmaßstab und ein Autonomiebegriff, der der folgenden Untersuchung zugrunde liegen soll, vorgestellt. An diese Vorarbeiten schließt der vierte Teil an, in dem untersucht wird, ob der nichtstaatliche Einsatz von Gesichtserkennungssystemen die Autonomie beeinträchtigt,

---

15 *O'Neil*, Weapons of Math Destruction; *Véliz*, Privacy is Power; *Zuboff*, The Age of Surveillance Capitalism; *Susser/Rössler/Nissenbaum*, Geo. L. Tech. Rev. 4:1 (2019), 1 (29 ff.); *Susser/Rössler/Nissenbaum*, Internet Policy Rev. 8:2 (2019), 1 (2).

16 *Frischmann/Selinger*, Re-Engineering Humanity, S. 271; *Zuboff*, The Age of Surveillance Capitalism, S. 347; *Susser/Rössler/Nissenbaum*, Geo. L. Tech. Rev. 4:1 (2019), 1 (34 ff.); *Susser/Rössler/Nissenbaum*, Internet Policy Rev. 8:2 (2019), 1 (3).

wobei zwischen Identifikations-, Verifikations- und Klassifizierungsverfahren differenziert wird. Sodann wird im fünften Teil untersucht, ob die betroffenen Personen vor den herausgearbeiteten Beeinträchtigungen durch das einfache Gesetz (ausreichend) geschützt werden. Im sechsten Teil wird der im April 2021 von der Kommission vorgestellte Verordnungsentwurf zur Regulierung Künstlicher Intelligenz mit Blick auf Gesichtserkennungssysteme untersucht.[17] Zum Schluss werden die wesentlichen Erkenntnisse zusammengefasst und es wird die Frage, ob eine Gefahr für die Autonomie besteht, beantwortet. Abschließend folgt ein rechtspolitischer Ausblick.

17 Europäische Kommission, 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, COM(2021) 206 final v. 21.4.2021.

Teil 1: Das menschliche Gesicht

Zunächst soll die Bedeutung des menschlichen Gesichts untersucht werden. Dabei soll zuerst auf die Einzigartigkeit des Gesichts eingegangen werden (A.) und sodann der Zusammenhang zwischen dem Gesicht und der Persönlichkeit dargestellt werden (B.). Daran anknüpfend sollen die vier am häufigsten vorkommenden Einsatzmethoden von Gesichtserkennungssystemen vorgestellt werden (C.) und schließlich soll untersucht werden, weshalb neben staatlichen Institutionen[18] auch nicht staatliche Stellen in den letzten Jahren ein zunehmendes Interesse am Zugriff auf menschliche Gesichtsdaten entwickelt haben (D.).

A. Die Einzigartigkeit des menschlichen Gesichts

Im Laufe der Evolution begünstigte ein starker Selektionsdruck die vielseitigen Variationen von Gesichtsmerkmalen.[19] Heute können Menschen sich am besten unter Heranziehung des Gesichts voneinander unterscheiden. Forscher der Universität Adelaide haben im Jahr 2015 herausgefunden, dass die Wahrscheinlichkeit, dass acht Gesichtsmerkmale bei zwei Personen identisch sind, bei über eins zu einer Billion liegt.[20] Bezieht man noch mehr Merkmale in den Abgleich ein, nimmt die Wahrscheinlichkeit weiter ab. Die Chance, dass man auf der Welt zwei Menschen mit exakt denselben Gesichtsmerkmalen findet, ist somit als äußerst gering einzuschätzen.

Anders als bei den üblichen Identifikationsmerkmalen, wie etwa dem Namen, der Adresse oder dem Geburtsdatum, kann es bei der Heranziehung der Gesichtsstruktur daher kaum zu Doppelungen und nur selten zu Verwechselungen kommen.

Ähnlich wie beim biometrischen Fingerabdruck, hat das Altern des menschlichen Körpers nahezu keinen Einfluss auf die Veränderung der

18 Siehe zum staatlichen Einsatz biometrischer Videoüberwachung *Schindler*, Biometrische Videoüberwachung.

19 *Sheehan/Nachman*, Nat. Commun. 5, Article number 4800 (2014), 1 (1 ff.).

20 *Lucas/Henneberg*, Forensic Sci. Int. *257* (2015), 514.e1 (514.e1 ff.).

biometrischen Gesichtsstruktur.[21] Trotz einer Veränderung der Haut oder einer Gewichtszunahme resp. -abnahme ist es möglich, Bildaufnahmen, die mit einem erheblichen zeitlichen Abstand zueinander aufgenommen worden sind, derselben Person zuzuordnen.[22] Dies macht den biometrischen Abdruck aufgrund seiner Einzigartigkeit über das gesamte Leben hinweg zu einem sicheren Erkennungsmerkmal. Biometrische Verfahren gelten zudem als besonders sicher, weil sie personalisiert sind und sich Dritte nicht ohne Weiteres mit ihnen ausweisen können. War es früher vorstellbar, dass eine Person einen fremden Ausweis einer Person, der sie ähnlich sah, vorzeigte oder einen fremden Transponder als Schlüssel verwendete, ist dies bei einer biometrischen Kontrolle nicht möglich. Vielmehr müsste der hinterlegte biometrische Abdruck verändert werden. Dies macht auch das Erstellen einer falschen Kopie deutlich komplizierter und mag manchen Missbrauch verhindern.

Dennoch birgt die hohe Sicherheit zugleich eine Gefahr: Werden die Daten des biometrischen Gesichtsabdrucks einer Person unberechtigter Weise erfasst und für rechtswidrige Zwecke verwendet, kann die betroffene Person ihre Gesichtsstruktur – zumindest ohne operativen Eingriff – nicht verändern.[23] Anders als bei herkömmlichen Ausweismöglichkeiten, wo die Zuordnungsnummer gesperrt werden kann und der betroffenen Person zum Beispiel ein neuer Ausweis ausgestellt oder ein neuer Transponder ausgegeben werden kann, ist es nicht möglich, einen neuen biometrischen Gesichtsabdruck zu erhalten.

B. Das Gesicht als Schlüssel zur Persönlichkeit

Das Gesicht als zentraler Teil des äußeren Erscheinungsbilds kann gleich aus mehreren Gründen Informationen über eine individuelle Person preisgeben. Sobald man den öffentlichen Raum betritt, zeigt man sein Gesicht. Das gilt nicht nur für den Auftritt in der Realität, sondern zunehmend auch für den virtuellen Raum. Anders als der Fingerabdruck, das Venenmuster der Hand oder die Netzhaut sind Gesichtsaufnahmen bereits überall vorhanden: Neben dem Personalausweis, Reisepass oder Führerschein

21 *Artikel-29-Datenschutzgruppe*, WP 80, S. 3.
22 *Artikel-29-Datenschutzgruppe*, WP 80, S. 3.
23 Zu Missbrauchsrisiken allgemein siehe auch *Lynch*, Face Off, S. 3; allgemein zur Gefahr des Identitätendiebstahls *Busch*, DuD 2009, 317; *Thiel*, ZRP 2016, 218 (221).

ist das Gesicht beispielsweise in sozialen Netzwerken, auf Unternehmenswebseiten oder auf online Dating-Portalen abgebildet.[24] Der visuelle Auftritt hat in den letzten Jahren enorm zugenommen. Mittlerweile nutzen über 54 Prozent der Menschen in Deutschland soziale Netzwerke wie etwa Facebook, Instagram oder Twitter.[25] Unter den 14- bis 29-jährigen sind es sogar 91 Prozent.[26] In dieser Altersklasse war die Foto-App Instagram in dem Zeitraum von 2018 bis 2021 das meistgenutzte soziale Netzwerk.[27] In den letzten Jahren konnte außerdem die Video-App TikTok auf dem deutschen Markt Fuß fassen und ihre Nutzerzahlen unter jungen Menschen stark ausbauen.[28] Möchte man wissen, wie das Gesicht einer bestimmten Person aussieht, muss man ihren Namen lediglich bei Google eingeben und findet in den meisten Fällen einen Treffer unter den ersten Vorschlägen der Suchmaschine, der nicht selten auf ein soziales Netzwerk verweist.

In der Öffentlichkeit kann man sein Gesicht der Wahrnehmung Dritter kaum entziehen. In vielen Gesellschaften gilt es als sozial ungewünscht, sein Gesicht zu verdecken, und es ist in bestimmten Situationen, wie etwa bei Demonstrationen, sogar verboten.[29]

Werden Bildaufnahmen von Personen gemacht, bekommt man diesen Vorgang in den meisten Fällen überhaupt nicht (mehr) mit, da Bildaufnahmen im öffentlichen Raum Teil des Alltags geworden sind. Nicht nur an öffentlichen Plätzen und im öffentlichen Nahverkehr werden Überwachungskameras eingesetzt, auch installieren immer mehr Unternehmen und Privatpersonen Aufnahmegeräte beispielsweise in Eingangsbereichen

---

24 *Garvie/Bedoya/Frankle*, The Perpetual Line-Up, S. 10.

25 Die Zahl bezieht sich auf das Jahr 2020, Europäische Kommission, eurostat, Personen, die das Internet zur Teilnahme an sozialen Netzwerken genutzt haben, abrufbar unter: https://ec.europa.eu/eurostat/databrowser/view/tin00127/default/table?lang=de.

26 Die Zahl bezieht sich auf das Jahr 2021, siehe ARD/ZDF-Onlinestudien, Social-Media-Nutzung 2018 bis 2021, abrufbar unter: https://www.ard-zdf-onlinestudie.de/social-media-und-messenger/social-media.

27 ARD/ZDF-Onlinestudien, Social-Media-Nutzung 2018 bis 2021, abrufbar unter: https://www.ard-zdf-onlinestudie.de/social-media-und-messenger/social-media.

28 Seven.One Media GmbH, ViewTime Report 2021, S. 22, abrufbar unter: https://www.seven.one/documents/924471/2568866/View+Time+Report+2021.pdf/8ae8af7c-3403-f495-0dad-5895a3095062?t=1635925222027.

29 Vgl. § 17a Abs. 2 Nr. 1 VersG. Wer gegen das sogenannte „Vermummungsverbot" verstößt kann gemäß § 27 Abs. 2 Nr. 2 VersG mit einer Freiheitsstrafe bis zu einem Jahr oder mit einer Geldstrafe bestraft werden oder muss gemäß § 29 Abs. 1 Nr. 1a VersG ein Bußgeld zahlen.