Das Verbot der Totalausforschung und seine digitale Zukunft

Nicolas Ziegler

A. Die Angst vor der Totalüberwachung

Die Totalüberwachung ist eine beliebte journalistische Projektion,[1] die auch jüngst im Rahmen des sog. Sicherheitspakets[2] der Bundesregierung als Reaktion auf den terroristischen Anschlag am 23.08.2024 in Solingen zur Bewertung konkreter sicherheitspolitischer Vorhaben eine Rolle gespielt hat.[3] Der Topos des totalen Überwachungsstaates rangiert zwischen den Polen einer historisch sensiblen deutschen Öffentlichkeit und einer aufmerksamkeitsökonomischen Verteidigung von Freiheitsrechten. Seit den 1970er-Jahren begleitet die Kritik am Überwachungsstaat die sicherheitsrechtlichen Debatten in Deutschland.[4]

I. Rezeption in Literatur und darstellender Kunst

Die Kritik an der Schaffung eines Überwachungsstaates findet sich ebenso in der darstellenden Kunst. Sowohl fiktionale Spielfilme wie „Minority Report", aber auch Werke mit realen Bezügen wie „Das Leben der Anderen" beschäftigen sich damit. Der Fixpunkt der literarischen Aufarbeitung des Themas ist und bleibt jedoch George Orwells Roman „1984".

1 Siehe nur *S. Krempl*, Faesers Fahndungsplan: Kritik an "Totalüberwachung des öffentlichen Raums", heise online v. 12.08.2024.

2 Hier allein von Interesse ist der Teil des Sicherheitspakets, der polizeiliche Ermittlungsbefugnisse ausweiten soll, Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung v. 09.09.2024, BT-Drs. 20/12806.

3 Vgl. den Überblick der Kritik bei *M. Reuter*, Massive Kritik am Sicherheitspaket der Ampel, netzpolitik.org. v. 11.09.2024.

4 *M. Kötter*, Pfade des Sicherheitsrechts, Baden-Baden 2008, S. 137 Fn. 694 m.w.N.

II. Rezeption in der Rechtswissenschaft

Während die Vergleichsfolie des orwellschen Überwachungsstaats in der politischen Argumentation ein legitimes Stilmittel sein kann, sollte die Rechtswissenschaft hierbei behutsamer vorgehen. Mit wenigen Ausnahmen[5] wird das juristische Schrifttum diesem Anspruch gerecht und zeichnet den Überwachungsstaat in der Regel nur als fernliegende Dystopie. Dennoch bringt die Literatur überwachungsstaatliche Dystopien in Verbindung mit konkreten Überwachungsmaßnahmen.[6] Über eine originelle Einleitung oder einen pointierten Schlusssatz hinaus vermag der Vergleich jedoch keinerlei Beitrag zur Fachdebatte zu leisten.[7]

III. Aufnahme des Topos durch das BVerfG

Auch das BVerfG hat sich in seiner Rechtsprechung bereits mit dem Überwachungsstaat oder vielmehr der totalen Überwachung auseinandergesetzt und klargestellt, dass eine Rundumüberwachung „von Verfassungs wegen stets unzulässig" ist.[8] Bei diesem Postulat ist es jedoch nicht geblieben und das BVerfG hat sich im Laufe seiner Rechtsprechung schon mehrfach zur Totalüberwachung geäußert, ohne jedoch den Inhalt und die Grenzen der Figur trennscharf zu bestimmen.

---

5 Besonders polemisch etwa *S. Schnorr*, Big Brother zur Verbrechensbekämpfung?, ZRP 2001, 291 (291 f.).

6 *D. Hauck*, Vorratsdatenspeicherung adé – hat ein orwellscher Albtraum vor dem BVerwG sein Ende gefunden?, jM 2024, 113*; M. Valta/J. Vasel,* Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz, ZRP 2021, 142 (143); *D. Uwer,* George Orwells „1984" – Antiutopie und Totalitarismuswarnung zwischen 1949 und 2009, NJW 2009, 723; BVerfG ZD 2018, 578 (582) m. Anm. *Kienle*; im Zusammenhang der Registermodernisierung *H. Bull,* Die Nummerierung der Bürger und die Angst vor dem Überwachungsstaat, DÖV 2022, 261.

7 *J. Schlömer*, Kontrollrechtliche Aspekte des Zugriffs von Nachrichtendiensten auf IT-Systeme, NVwZ 2023, 1121 (1127); *H. Bull,* Fehlentwicklungen im Datenschutz am Beispiel der Videoüberwachung, JZ 2017, 797 (797).

8 BVerfGE 112, 304 (319).

B. Das Totalüberwachungsverbot als Figur der verfassungsrechtlichen Dogmatik

Das sog. Totalüberwachungsverbot, synonym oft auch als Verbot der Rundumüberwachung bezeichnet, findet sich erstmals im Urteil des BVerfG zum großen Lauschangriff von 2004.[9] Das BVerfG entwickelt dieses Verbot in folgender Passage: „Die Menschenwürde wird auch verletzt, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können".[10] Damit formuliert das Gericht eine spezifisch sicherheitsrechtliche rote Linie für staatliche Informationseingriffe.[11] Nachfolgend sollen zunächst die Entwicklungslinien bis zu diesem Urteil nachgezeichnet werden (I.), ehe das Totalüberwachungsverbot als eigenständige verfassungsrechtsdogmatische Figur beleuchtet werden soll (II.).

I. Vorarbeiten: Die Gefahr der Bildung von Persönlichkeitsprofilen in der Rechtsprechung des BVerfG

Dass eine vollkommene und umfassende Überwachung nicht mit der Verfassungsordnung des GG vereinbar sein kann, lässt sich der Rechtsprechung des BVerfG bereits vor der eben dargestellten expliziten Ausformulierung entnehmen. Bereits nach der Objektformel Dürigs, die das BVerfG in seine Rechtsprechung als negative Definition der Menschenwürde i.S.v. Art. 1 Abs. 1 GG übernommen hat,[12] wird die Menschenwürde verletzt, wenn „der konkrete Mensch zum Objekt, zu einem bloßen Mittel, zur vertretbaren Größe herabgewürdigt wird".[13] Die Herabwürdigung des Menschen zum bloßen Objekt staatlicher Datenverarbeitung nimmt das BVerfG

9 BVerfGE 109, 279.

10 BVerfGE 109, 279 (323).

11 Der Begriff der staatlichen Informationseingriffe fasst den sicherheitsbehördlichen Umgang mit Informationen eingriffs- und grundrechtsunabhängig bzw. übergreifend zusammen, vgl. zum Informationseingriff und seiner terminologischen Verwendung durch das BVerfG, *S. Tannenberger*, Die Sicherheitsverfassung, Tübingen 2014, S. 225 ff.

12 *T. Linke*, Die Menschenwürde im Überblick: Konstitutionsprinzip, Grundrecht, Schutzpflicht, JuS 2016, 888 (890 f.).

13 *G. Dürig*, Der Grundsatz von der Menschenwürde, AöR 81 (1956), 117 (127).

im Mikrozensus-Beschluss auf. Es konkretisiert den Verstoß dahingehend, dass es mit der Menschenwürde nicht zu vereinbaren ist, „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren".[14] Damit steht bereits früh fest, dass die Bildung eines umfassenden Persönlichkeitsprofils einen Verstoß gegen Art. 1 Abs. 1 GG bedeutet. Von dieser Annahme, dass Menschen „einer Bestandsaufnahme in jeder Beziehung" verfassungsrechtlich nicht zugänglich sind,[15] ist es nur ein kleiner Schritt zum Schutz des Innenraums, der einem „um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen […] verbleiben muß".[16] Der menschenrechtswürdekonforme Schlusspunkt staatlicher Datenverarbeitung, das Persönlichkeitsprofil, hat sich ausgehend vom noch rudimentären Privatheitsschutz im Elfes-Urteil[17] und dem Mikrozensus-Beschluss[18] auch bei der Entwicklung des Rechts auf informationelle Selbstbestimmung im Volkszählungsurteil gehalten.[19] Was genau unter einem solchen umfassenden Persönlichkeitsbild verstanden werden kann, ist bis heute jedoch unklar.[20] Das BVerfG hat es bisher dabei bewenden lassen, lediglich vor der Gefahr solcher zu warnen.[21] Derartige Persönlichkeitsprofile dürfen nicht mit Profilen i.S.v. Art. 3 Nr. 4 JI-RL verwechselt werden, die nur „bestimmte persönliche Aspekte" betreffen.

II. Anerkennung als eigene dogmatische Figur

Das geschriebene Verfassungsrecht kennt nur wenige absolute und abwägungsfeste Grenzen für Grundrechtseingriffe. Hierzu zählt das Rückwirkungsverbot aus Art. 103 Abs. 2 GG, der Wesensgehalt der Grundrechte nach Art. 19 Abs. 2 GG und die Menschenwürdegarantie des Art. 1 Abs. 1

14 BVerfGE 27, 1 (6).
15 BVerfGE 27, 1 (6).
16 BVerfGE 27, 1 (5 f.).
17 BVerfGE 6, 32 (41).
18 BVerfGE 27, 1 (6).
19 BVerfGE 65, 1 (52 f.): Trotz der Weiterentwicklung des Privatheitsschutzes unter dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und seiner Ausprägung des Rechts auf informationeller Selbstbestimmung bleibt die „umfassende […] Katalogisierung der Persönlichkeit" in der Menschenwürde verankert.
20 Pionierarbeit leistet hier *C. Conrad*, Ein Update für den Kernbereichsschutz, Berlin 2024, S. 19 ff.
21 Zuletzt BVerfGE 141, 220 (280 Rn. 130); 156, 63 (123 Rn. 210).

GG.[22] Die Menschenwürde ist dabei aber in höchstem Maße offen und auslegungsbedürftig. Für das Sicherheitsrecht haben sich hier der Schutz des Kernbereichs privater Lebensgestaltung[23] und das Totalüberwachungsverbot[24] als absoluten Grenzen herauskristallisiert.

1. Menschenwürdeverstoß durch Rundumüberwachung

Seit der ersten Entwicklung des Totalüberwachungsverbots im Urteil zum großen Lauschangriff hat das BVerfG diese Figur, die es aus dem bereits im Volkszählungsurteil formulierten Risiko der Bildung von Persönlichkeitsprofilen zieht,[25] mehrfach wieder aufgegriffen. Bereits ein Jahr nach der ersten Konkretisierung betont das BVerfG in seiner Entscheidung zur GPS-Überwachung, dass eine Rundumüberwachung von Verfassungs wegen stets unzulässig ist.[26] Anders als beim Schutz des Kernbereichs privater Lebensgestaltung bedarf es aber keiner verfahrensrechtlichen Absicherung gegen einen Verstoß.[27] Im Urteil zur Vorratsdatenspeicherung warnt das BVerfG davor, dass eine anlasslose und massenhafte Speicherung von Telekommunikationsverkehrsdaten „als Schritt hin zu einer" Rundumüberwachung verstanden werden könnte.[28] Auch hier knüpft das BVerfG an das umfassende Persönlichkeitsprofil an, das es zu verhindern gilt.[29] Gleichzeitig stellt das BVerfG fest, dass das Totalüberwachungsverbot zur verfassungsrechtlichen Identität der Bundesrepublik i.S.v Art. 79 Abs. 3 GG zählt.[30] Im Jahr 2011 prüfte das BVerfG erstmals, ob eine konkrete akustische Wohnraumüberwachung gegen das Totalüberwachungsverbot versto-

22 Zur Unabwägbarkeit der Menschenwürde *F. Wapler*, in: H. Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. I, 4. Aufl., Tübingen 2023, Art. 1 Abs. 1 Rn. 95 m.w.N.

23 Zur dogmatischen Einordnung *M. Eichberger*, in: P. Huber/A. Voßkuhle (Hrsg.), Grundgesetz-Kommentar, Bd. I, 8. Aufl., München 2024, Art. 2 Rn. 159 ff.

24 *I. Dammann*, Der Kernbereich der privaten Lebensgestaltung, Berlin 2011, S. 152; *C. Rottmeier*, Kernbereich privater Lebensgestaltung und strafprozessuale Lauschangriffe, Tübingen 2017, S. 137.

25 BVerfGE 65, 1 (42 f.) worauf BVerfGE 109, 279 (323) verweist.

26 BVerfGE 112, 304 (319).

27 BVerfGE 112, 304 (319 f.).

28 BVerfGE 125, 260 (323 f.).

29 BVerfGE 125, 260 (324): „Sie [die Vorratsdatenspeicherung] darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen".

30 BVerfGE 125, 260 (324); bestätigt durch BVerfGE 156, 63 (123 Rn. 210).

ßen hat.[31] Im BKAG-Urteil von 2016 wiederholt das BVerfG das Verbot der Rundumüberwachung,[32] während es vorerst letztmalig im Beschluss vom 01.12.2020 zur elektronischen Aufenthaltsüberwachung thematisiert wird, in welchem das BVerfG herausarbeitet, dass die dauerhafte Bestimmung des Aufenthaltsortes alleine den Betroffenen noch nicht zum bloßen Objekt staatlichen Handelns macht.[33]

Auffallend ist dabei, dass die Thematisierung des Totalüberwachungsverbots durch das BVerfG durchgängig eine hohe sprachliche Konsistenz aufweist und eine Weiterentwicklung oder Schärfung der Konturen unterbleibt. Abstrakte Aussagen über das bloße Postulat des Verbots einer Totalüberwachung hinaus können nicht getroffen werden und eine praktische Handhabung gelingt nur entlang der Natur des Einzelfalls.[34]

2. Konturen des Tatbestands der Rundumüberwachung

Betrachtet man die eben genannten Urteile, lassen sich zwei Orientierungspunkte erkennen. *Erstens* sind die Eingriffsmodalitäten, konkret der Umfang und die Dauer einer Überwachung und nicht Inhalte oder Qualität vorrangige Parameter für die Prüfung.[35] *Zweitens* ist diese quantitative Betrachtung dahingehend zu überprüfen, ob sich aus den gesammelten Daten die Gefahr der Bildung eines Persönlichkeitsprofils ergibt.[36] Damit weist das Totalüberwachungsverbot nur wenig Konturen auf. Mit Blick auf die Eignung eines konkreten Datensatzes zur Bildung eines Persönlichkeitsprofils gibt es aber zumindest ein Kriterium für die Handhabung im Einzelfall. Vorhersagbar sind die Ergebnisse einer Prüfung damit jedoch nicht: Die Meinungen darüber, ob das Totalüberwachungsverbot im Einzelfall verletzt sein wird, werden stark divergieren und der eigentliche Vorteil einer absoluten Grenze für staatliche Informationseingriffe, die Rechtssicherheit,[37] kann nicht erreicht werden.

31 BVerfGE 130, 1 (24).
32 BVerfGE 141, 220 (280 Rn. 130).
33 BVerfGE 156, 63 (136 Rn. 251).
34 *T. Schwabenbauer*, Heimliche Grundrechtseingriffe, Tübingen 2013, S. 295.
35 *Schwabenbauer*, Grundrechtseingriffe (Fn. 34), S. 293; *Tanneberger*, Sicherheitsverfassung (Fn. 11), S. 136.
36 *F. Nicolai*, Das Internet der Dinge und das Strafrecht, Berlin 2024, S. 290 f.
37 *Schwabenbauer*, Grundrechtseingriffe, (Fn. 34), S. 253 m.w.N.

3. Abgrenzung

Aufgrund der Konturlosigkeit stellt sich die Frage, ob das Totalüberwachungsverbot tatsächlich eine eigenständige dogmatische Figur des BVerfG ist, oder nicht vielmehr die spezifische Subsumtion umfangreicher Überwachung unter andere dogmatische Schutzkonzepte der Privatheit. Aufgrund der Einzelfallfokussierung ist das Totalüberwachungsverbot jedenfalls keine bloße Warnung an den Sicherheitsgesetzgeber.[38]

a) Schutz des Kernbereichs privater Lebensgestaltung

Häufig wird ausgehend von einer missverstandenen Aussage des BVerfG[39] vertreten, dass das Totalüberwachungsverbot lediglich eine „Verletzungsmodalität" des Kernbereichs privater Lebensgestaltung ist.[40] Der Wortlaut („regelmäßig") legt hier jedoch nahe, dass eine Verletzung des Totalüberwachungsverbots auch möglich ist, wenn Daten ohne höchstpersönlichen Bezug zu einem Persönlichkeitsprofil zusammengesetzt werden.[41] Gleichwohl stellt ein Persönlichkeitsprofil, auch wenn es ohne jeden Kernbereichsbezug erstellt wurde, selbst eine kernbereichsrelevante Information dar, schließlich lässt sich aus großen Mengen von vermeintlich belanglosen Daten Höchstpersönliches rekonstruieren.[42] Eine Abgrenzung ist also nicht trivial.

38 So ist vielmehr die sog. Überwachungsgesamtrechnung zu verstehen, *J. Lindner/J. Unterreitmeier*, »Überwachungsgesamtrechnung«: Karlsruhe calculat?, JZ 2022, 915 (915).

39 BVerfGE 109, 279 (323): „Eine zeitliche und räumliche `Rundumüberwachung´ wird regelmäßig schon deshalb unzulässig sein, weil die Wahrscheinlichkeit groß ist, dass dabei höchstpersönliche Gespräche abgehört werden".

40 *M. Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, Baden-Baden, 2007, S. 65; ähnlich *Tanneberger*, Sicherheitsverfassung (Fn. 11), S. 259; *T. Bode*, Verdeckte strafprozessuale Ermittlungsmaßnahmen, Berlin 2012, S. 162.

41 *Rottmeier*, Lauschangriffe (Fn. 24), S. 137.

42 *Conrad*, Kernbereichsschutz (Fn. 20), S. 30 ff.; vgl. BVerfGE 65, 1 (45): es gibt „kein „belangloses" Datum mehr".

b) Recht auf informationelle Selbstbestimmung

Auch wenn das Recht auf informationelle Selbstbestimmung Menschenwürdebezug aufweist, das Totalüberwachungsverbot ist ein „selbstständiger Menschenwürdeverstoß".[43] Die erforderliche Trennung der beiden Gewährleistungen fällt hier aber ebenfalls nicht leicht, da das BVerfG bislang nicht erklärt hat, wann es staatliche Informationseingriffe „nur" an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG misst und wann die Prüfung alleine an Art. 1 Abs. 1 GG erfolgt. Die Abgrenzung wird nach der Konzeption des Totalüberwachungsverbots durch das BVerfG quantitativ vorgenommen: Die sicherheitsbehördliche Datenverarbeitung misst sich so lange am Recht auf informationelle Selbstbestimmung, bis ausreichend Daten vorhanden sind, mit denen man ein Persönlichkeitsprofil erstellen könnte.[44] Die Festlegung, „welche Maßnahme diejenige sein soll, die als sprichwörtlicher Tropfen das Fass zum Überlaufen bringt"[45] erweist sich im Einzelfall aber als schwierig. Aufgrund der Relationalität von Daten darf man sich das Verhältnis vom Eingriff in das Recht auf informationelle Selbstbestimmung und der verbotenen Totalüberwachung aber nicht als bloße lineare Entwicklung vorstellen.

C. Herausforderungen für das Totalüberwachungsverbot

Trotz der dogmatischen Schwierigkeiten und der nur geringen Praxisrelevanz des Totalüberwachungsverbots wird dessen Bedeutung im Rahmen der Digitalisierung sicherheitsbehördlicher Ermittlungsarbeit zunehmen. Schon heute fordern digitale Sachverhalte[46] das Verbot einer Rundumüberwachung heraus. Dies zeigen die nachfolgenden Szenarien.

43 *Eichberger* (Fn. 23), Art. 2 Rn. 315.

44 Ähnlich grenzt sich auch das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme von der informationellen Selbstbestimmung ab, vgl. *H. Gersdorf*, in: H. Gersdorf/B. Paal (Hrsg.), BeckOK InfoMedienR, 42. Ed. v. 1.5.2021, München, GG Art. 2 Rn. 25.

45 *G. Hornung*, Die kumulative Wirkung von Überwachungsmaßnahmen, in: M. Albers/R. Weinzierl (Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik, Baden-Baden 2010, S. 65 (73).

46 Begriffsbildend zum digitalen Sachverhalt *S. Rachut*, Grundrechtsverwirklichung in digitalen Kontexten, Berlin 2024 (i.E.), S. 169–208, insb. S. 200.

I. Ermittlungen im Metaverse

Vorhersagen zufolge wird bereits 2026 ein Viertel der Weltbevölkerung mindestens eine Stunde täglich im sog. Metaverse[47] verbringen.[48] Wie bei jeder technischen Innovation hat auch hier schon eine Instrumentalisierung durch Kriminelle eingesetzt, die sog. Metacrimes begehen.[49] Um dieser Kriminalität zu begegnen, gibt es Einsatzfelder von Virtual Reality (VR) für Sicherheitsbehörden, die rechtlich wenige Probleme aufwerfen.[50] Hierzu zählen etwa virtuelle Streifengänge der Polizei an Spawnpunkten[51] oder der Einsatz von VR als forensische Medientechnik durch begehbare 3D Modelle von Tatorten.[52]

Ein Problem für das Totalüberwachungsverbot oder vielmehr die Bildung von Persönlichkeitsprofilen stellt jedoch die große Menge sensibler Daten dar, die verarbeitet werden.[53] Durch Datenbrillen und andere sensorisch ausgestattete Hardware zur Interaktion sowie einem umfassend realistisch nachgebildeten Avatar der Nutzer gibt es wohl keinen anderen Bereich, „in dem so unmittelbar personenbezogene Daten abgegriffen werden können".[54] Diese Fülle an Daten ermöglicht ein tiefes Eindringen in die Persönlichkeit Betroffener und macht diese in ihrem Verhalten vorhersehbar.[55] Veranschaulicht werden kann das durch beim Gaming aufgezeichnete Interaktion und Entscheidungsfindung, die tiefe Einblicke in die

47 Verstanden als virtueller Raum, vgl. zu den Merkmalen und unterschiedlichen Immersionsgraden ausführlich bei *M. Kaulartz/A. Schmid/F. Müller-Eising,* Das Metaverse – eine rechtliche Einführung, RDi 2022, 521 (522 f.).

48 Interpol, Metaverse: A Law Enforcement Perspective, White Paper, Januar 2024, S. 5.

49 Begriff und eine Übersicht zu möglichen Deliktsfeldern bei Interpol, Metaverse: A Law Enforcement Perspective, White Paper, Januar 2024, S. 11 ff.

50 *E. Hilgendorf*, Virtuelle Realitäten, Metaverse, Generative KI und (Straf-)Recht, JZ 2024, 677 (686).

51 So der Vorschlag von *M. Martini/J. Botta,* Der Staat und das Metaversum, MMR 2023, 887 (897).

52 Siehe zum Holodeck des bayerischen Landeskriminalamts *R. Breker*, Holodeck – Das VR-Lab der bayerischen Polizei, Kriminalistik 2024, 130.

53 Siehe zur Fülle sensibler und biometrischer Daten bei *Martini/Botta,* Metaversum (Fn. 51), 894.

54 *Hilgendorf,* Realitäten (Fn. 50), 683.

55 Zur Persönlichkeitsrelevanz von Big Data allgemein *M. Martini*, Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl 2014, 1481. Spezifisch für das Metaverse *Hilgendorf,* Realitäten (Fn. 50), 683.

Persönlichkeit ermöglicht.[56] Die Avatare im Metaverse können von ihrer Persönlichkeitsrelevanz daher im wahrsten Sinne des Wortes als digitale Zwillinge bezeichnet werden, weshalb bei ihrer Einbeziehung in Ermittlungen äußerst behutsam vorzugehen ist.

II. Biometrische Identifizierung

Videoüberwachung im öffentlichen Raum zu präventiven Zwecken ist inzwischen weit verbreitet und wird in der Rechtswissenschaft schon lange intensiv diskutiert.[57] Umfassende Videoüberwachung ruft zielsicher die bereits oben thematisierten Orwell-Vergleiche hervor.[58] Kombiniert man Videoüberwachung oder großflächiges Web Scraping[59] mit KI-gestützter Gesichtserkennung, hat dies das Potenzial, Anonymität im (digitalen) öffentlichen Raum aufzuheben, weshalb eine Betrachtung aus der Perspektive des Totalüberwachungsverbots lohnt.[60] An dieser Stelle kann und soll daher keine vertiefte verfassungsrechtliche Analyse der Zulässigkeit von Gesichtserkennung erfolgen.[61] Vielmehr soll der Einsatz dieser Technik – sofern er mit Rechtsgrundlagen legitimiert wird – auf seine Gefahr zur Bildung umfassender Persönlichkeitsprofile hin untersucht werden.

1. Begriff und aktuelle sicherheitspolitische Vorhaben

Sowohl die biometrische Echtzeit-Fernidentifizierung als auch die nachträgliche biometrische Fernidentifizierung sollen hier beleuchtet werden. Als Oberbegriff kann die biometrische Identifizierung gebildet werden.

56 *C. Geminn,* Deus ex machina?, Tübingen 2023, S. 262 mit weiterführenden empirischen Nachweisen in Fn. 404.
57 *T. Starnecker*, Videoüberwachung zur Risikovorsorge, Berlin 2017, S. 21 ff.
58 Siehe nur *J. Käppner*, Beobachtet von tausend Augen, SZ v. 17.12.2018.
59 Hierunter versteht man die automatisierte Extraktion von Informationen auf frei verfügbaren Webseiten.
60 So auch *M. Martini*, Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit, NVwZ-Extra 1–2/2022, 1 (4, 7 f.), der die Totalüberwachung als „rote Linie" der Gesichtserkennung bezeichnet; i.E. ähnlich *G. Hornung/S. Schneider*, Das biometrische Auge der Polizei, ZD 2017, 203 (206).
61 Siehe hierzu bei *A. Heldt,* Gesichtserkennung: Schlüssel oder Spitzel?, MMR 2019, 285; *Martini*, Gesichtserkennung (Fn. 60), 5 ff.

Da es hierfür keine allgemein anerkannte Definition gibt,[62] greift dieser Beitrag der Einfachheit halber auf die Legaldefinition der biometrischen Identifizierung in Art. 3 Nr. 35 KI-VO zurück.[63] Intelligente Gesichtserkennung funktioniert über den Abgleich biometrischer Merkmale des Gesichts durch neuronale Netze mit vorhandenen Bilddaten und erbringt Leistungen, die dem Menschen durch manuellen Vergleich nicht möglich wäre.[64] Zwischen den beiden Varianten der biometrischen Identifikation kann folgendermaßen abgegrenzt werden: Die Echtzeit-Fernidentifizierung wird durch Videoüberwachung realisiert, während die nachträgliche Fernidentifizierung – für den Blickwinkel dieses Beitrags – ein biometrisches Web Scraping darstellt. Vereinzelt kam es in Deutschland schon zum präventiven[65] und repressiven[66] Einsatz von Gesichtserkennungssoftware durch Sicherheitsbehörden. Nicht zuletzt aufgrund der massiven Kritik an dieser Verwendung einigten sich die die Bundesregierung tragenden Parteien 2021 darauf, auf „flächendeckende Videoüberwachung und den Einsatz von biometrischer Erfassung zu Überwachungszwecken" zu verzichten.[67] Genau dies plant nun aber das BMI.[68] Mit einem Referentenentwurf, der allerdings auf eine Echtzeit-Fernidentifikation verzichtet,[69] will das BMI mit §§ 10b, 39a, 63b BKAG-E, § 34b BPolG-E und § 98d StPO-E den retrograden biometrischen Abgleich polizeilicher Datenbanken mit dem

62 Für die biometrische Fernidentifizierung *J. Hahn*, Die Regulierung biometrischer Fernidentifizierung in der Strafverfolgung im KI-Verordnungsentwurf der EU-Kommission, ZfDR 2023, 142 (145).

63 Nach Art. 3 Nr. 35 KI-VO ist eine biometrische Identifizierung „die automatisierte Erkennung physischer, physiologischer, verhaltensbezogener oder psychologischer menschlicher Merkmale zum Zwecke der Feststellung der Identität einer natürlichen Person durch den Vergleich biometrischer Daten dieser Person mit biometrischen Daten von Personen, die in einer Datenbank gespeichert sind".

64 *B. Kees*, Algorithmisches Panopticon, Münster 2015, S. 17 f.

65 Test der Bundespolizei am Bahnhof Berlin Südkreuz von 2017–2018, Bundespolizei, Test zur Gesichtserkennung am Bahnhof Berlin Südkreuz gestartet, Pressemitteilung v. 10.8.2017.

66 Im Rahmen der Strafverfolgung nach dem G20 Gipfel 2017 im Hamburg, vgl. VG Hamburg, Urt. v. 23.10.2019 – 17 K 203/19, BeckRS 2019, 40195.

67 SPD/Grüne/FDP, Mehr Fortschritt wagen, Koalitionsvertrag v. 24.11.2021, S. 109.

68 Referentenentwurf des BMI v. 06.08.2024, veröffentlicht durch *A. Meister*, Wir veröffentlichen den Entwurf zum neuem BKA-Gesetz, netzpolitik.org v. 15.08.2024. Nach anfänglich heftiger Kritik auch in Koalitionskreisen als Teil des sog. Sicherheitspakets nach dem Solingen-Attentat durch BT-Drs. 20/12806 als Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung eingebracht.

69 Im Sinne von Art. 3 Nr. 42 KI-VO und dem korrespondierenden Verbot in Art. 5 Abs. 1 lit. h KI-VO.

gesamten Internet ermöglichen. Damit würde dem Staat erlaubt werden, was Unternehmen wie ClearviewAI und Pim Eyes bereits realisiert haben.[70]

2. Exkurs: KI-VO als Zulässigkeitsdeterminante biometrischer Abgleiche

Die KI-VO[71] regelt auch die biometrische Echtzeit-Fernidentifizierung durch Videoüberwachung. Sie ordnet biometrische Echtzeit-Fernidentifizierungssysteme im öffentlichen Raum zu Strafverfolgungszwecken im Rahmen ihres risikobezogenen Regulierungsansatzes nach Art. 5 Abs. 1 lit. h KI-VO als KI-System mit einem unannehmbaren Risiko ein, das in einem unauflöslichen Widerspruch zu den Werten der Union steht und daher grds. verboten ist.[72] Zentraler Kritikpunkt am Verbot ist die eher offen formulierte Liste an Ausnahmen, die im Ergebnis „ein äußerst aufgeweichtes Verbot" schaffe.[73] Letztendlich wurde aus dem Verbot eine Öffnungsklausel für videobasierte Gesichtserkennung im Rahmen der Anforderungen von Art. 5 Abs. 2 ff. KI-VO.[74] Für retrograde Gesichtserkennung im Wege eines Abgleichs mit öffentlich zugänglichen Informationen aus dem Internet wie etwa Social-Media-Profilen verbietet Art. 5 Abs. 1 lit. e KI-VO aber eine notwendige technische Vorstufe zum Abgleich:[75] die Erstellung einer biometrischen Referenzdatenbank. Dieses Verbot ist deutlich weniger flexibel, da es offensichtlich auf das Verbot von Geschäftspraktiken von Unternehmen wie ClearviewAI zielt.[76]

---

70 Umfassend bei *M. Martini/C. Kemper,* Clearview AI: das Ende der Anonymität? Teil 1: Zulässigkeit der App, CR 2023, 341 (341 f.).

71 VO (EU) 2024/1689, ABl. L v. 12.07.2024.

72 Siehe zum risikobasierten Verbot *P. Bronner*, Risikoklassifizierung, Risikobewertung und Risikominimierung nach der KI-Verordnung, KIR 2024, 55 (57 f.).

73 *F. Rostalski/E. Weiss*, Verbotene KI-Praktiken (Art. 5 KI-VO-E), in: E. Hilgendorf/D. Roth-Isigkeit (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz, München, 2023, § 3 Rn. 15.

74 *J. Ganter/J. Rembold,* in: R. Schwartmann/T. Keber/K. Zenner (Hrsg.), KI-VO, Heidelberg, 2024, 2. Teil 1. Kapitel Rn. 100 ff., 118.; *D. Bomhard/ J. Siglmüller*, AI Act – das Trilogergebnis, RDi 2024, 45 (48) weisen auf die Redundanz bzw. den bloßen Signalcharakter der Verbote hin. In diesem Zusammenhang ist Art. 10 und 11 JI-RL zu sehen. Zu deren Voraussetzungen an Gesichtserkennung *Martini*, Gesichtserkennung (Fn. 60), 5 f.

75 Ohne eine solche Referenzdatenbank aus sämtlichen öffentlich zugänglichen Bild-, Videoerzeugnissen und Stimmaufzeichnungen, müsste jeder Abgleich mit dem Gesamtbestand des Internets durchgeführt werden.

76 Die Datenbank beläuft sich laut eigenen Angaben auf über 50 Milliarden Bilder, https://www.clearview.ai.

3. Persönlichkeitsprofilbildung durch die Überwachung des (digitalen) öffentlichen Raums?

Das Recht auf informationelle Selbstbestimmung garantiert auch Anonymität im öffentlichen Raum.[77] Sowohl die Erfassung des menschlichen Gesichts als biometrisches Datum als auch die Durchführung eines Datenabgleichs bedeuten einen Eingriff in den Schutzbereich der informationellen Selbstbestimmung.[78] Die Gefahr der Persönlichkeitsprofilbildung markiert das sprichwörtliche Überlaufen des Fasses der Eingriffe in die informationelle Selbstbestimmung zum selbstständigen Menschenwürdeverstoß der Totalüberwachung.[79]

a) Stationäre Gesichtserkennung

Ob die Kombination stationärer Videoüberwachung mit KI-gestützter Gesichtserkennung die Bildung umfassender Persönlichkeitsprofile ermöglicht oder bei einer Kumulation mit weiteren Maßnahmen dazu beitragen kann, ist maßgeblich von der Installationsdichte der Überwachungskameras im öffentlichen Raum abhängig.[80] Je nach Anordnung und Anzahl der Kameras lassen sich engmaschige Bewegungsprofile erstellen, die wiederum weitreichende Rückschlüsse auf das Privat- und Sozialleben ermöglichen.[81] Zu Recht betont daher das BVerfG in seinen Entscheidungen zum Totalüberwachungsverbot, dass eine weitreichende Aufzeichnung der Bewegungen eines Menschen ein substanzieller Teil eines Persönlichkeitsprofils sein kann.[82] Wo die genaue Grenze zum selbstständigen Menschen-

77 BVerfGE 120, 378 (399 f.).

78 *Heldt,* Gesichtserkennung (Fn. 61), 287; BVerfGE 150, 244 (266 Rn. 43 ff.) für die automatisierte Kennzeichenerfassung.

79 Siehe schon bei B. II. 2.

80 *Hornung/Schneider*, Biometrisches Auge (Fn. 60), 206; vgl. zur Überwachungsdichte die Anzahl der Überwachungskameras je 1.000 Einwohner, Statista, Big Brother is watching you, https://de.statista.com/infografik/22350/ueberwachunsgkameras-in-ausgewaehlten-grossstaedten/ (zuletzt abgerufen am 28.09.2024).

81 Sogar sensible Informationen über sexuelle Präferenzen, Religion oder Gesundheitsprobleme können daraus abgeleitet werden, EDSA, Leitlinien 05/2022, Version 2.0 v. 26.04.2023, S. 16, 57; *K. Lachmayer*, Grundrechtliche Implikationen von Videoaufzeichnungen im öffentlichen Raum, NLMR 2023, 203 (210); *Hahn,* Fernidentifizierung (Fn. 62), 143.

82 BVerfGE 109, 279 (323); 130, 1 (24). Weniger problembewusst bzgl. der elektronischen Aufenthaltsüberwachung jedoch BVerfGE 156, 63 (136 Rn. 250 f.).

würdeverstoß liegt, wird sich aber nur im Einzelfall beurteilen lassen. Im Vergleich zu chinesischen und britischen Verhältnissen[83] werden Bewegungsprofile durch intelligente Videoüberwachung in Deutschland wohl noch länger allein ein Problem für das Recht auf informationelle Selbstbestimmung bleiben. Klar ist aber: Aus umfassenden Bewegungsprofilen lassen sich durch moderne Analysemethoden Persönlichkeitsprofile bilden.

b) Biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

Während Kameraüberwachung den öffentlichen Raum im geografisch-analogen Sinne vermessen kann, ermöglicht ein biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet eine detaillierte Vermessung des digitalen öffentlichen Raums. Bedenkt man die Fülle an Foto- und Videoaufnahmen auf Social-Media-Plattformen, auf deren Auswertung die Maßnahmen abzielen, „findet bereits jetzt eine weitreichende bildliche Dokumentation unseres Alltags im Internet statt – Tendenz steigend".[84] Mit dieser biometrisch genauen Lupe lässt sich das gesamte Bildmaterial einer Person im öffentlichen Internet finden und anschließend auswerten. Gerade bei digital freizügigeren Personen ergibt sich schnell eine Datenmenge, die eine Gefahr zur Bildung von Persönlichkeitsprofilen begründen kann. Drastisch formuliert könnten „die Handys der Bürger:innen in Zukunft […] immer auch als Überwachungskameras des Staates verwendet" werden.[85] Abstrakte Konturen für das Totalüberwachungsverbot des BVerfG lassen sich hier aber keine entwickeln. Wann es zu einer konkreten Gefahr der Bildung von Persönlichkeitsprofilen kommt, kann nur in einer Einzelfallbetrachtung ermittelt werden. Die vorgeschlagenen Rechtsgrundlagen der §§ 10b, 39a und 63b BKAG-E begründen aufgrund der mangelnden Begrenzung der Datenmengen,[86] der anwendbaren Methoden und der pau-

83 *D. Boffey*, Britain is 'omni-surveillance' society, watchdog warns, The Guardian v. 29.10.2023.

84 *N. Härting/L. Voigt/D. Albrecht*, Anwaltverein sieht „Verfassungsbeschwerde garantiert", netzpolitik.org v. 30.08.2024.

85 *E. Tuchtfeld*, D64 kritisiert Pläne von Faeser, Pressemittelung v. 12.08.2024, abrufbar unter https://d-64.org/plaene-faeser/ (zuletzt abgerufen am 10.10.2024).

86 Die Sicherheitsbehörden könnten aufgrund der Konturlosigkeit und Technikoffenheit der vorgeschlagenen Rechtsgrundlagen dazu verleitet werden, eine oben bereits thematisierte biometrische Referenzdatenbank anzulegen.

schalen Bezugnahme auf sämtliche Daten, auf die das BKA zugreifen darf, allerdings bereits eine abstrakte Gefahr der Bildung von Persönlichkeitsprofilen.[87]

III. Überblick weiterer Problemfelder

Neben den dargestellten eher neuen Phänomenen der Sicherheitsgewährleistung regt das Totalüberwachungsverbot aber auch zum Nachdenken über Ermittlungsmaßnahmen an, die die sicherheitsrechtliche Debatte schon länger prägen.

1. Online-Durchsuchung

Das Totalüberwachungsverbot entwickelt gerade bei kumulativer Überwachung eine besondere Bedeutung.[88] Die Online-Durchsuchung stellt aber eine Maßnahme dar, die schon für sich allein betrachtet eine derart große Menge an Daten erhebt, dass bei deren Verknüpfung die Gefahr der Bildung von Persönlichkeitsprofilen besteht.[89] Je nach Gerät und der Intensität seiner Nutzung ermöglicht eine Onlinedurchsuchung, der Zielperson „beim Denken" zuzusehen.[90] Sogar etablierte – wenn auch nicht unumstrittene – und verfassungsgerichtlich bereits näher ausgeleuchtete Maßnahmen wie die Online-Durchsuchung können das Totalüberwachungsverbot daher im Einzelfall verletzen. Hauptgrund hierfür ist ein eher an punktuellen inhaltlich-qualitativen Verletzungen orientierter Kernbereichsschutz, der die Gefahr von Persönlichkeitsprofilen nicht adressiert.[91]

87 Angesichts der ermöglichten umfassenden Datensammlung fällt das Ausklammern von Informationen aus Online-Durchsuchungen und akustischer Wohnraumüberwachung nach § 10b Abs. 3 S. 2 BKAG-E i.V.m. § 12 Abs. 3 BKAG hier kaum ins Gewicht.

88 Weshalb es auch einer Abgrenzung zum sog. additiven Grundrechtseingriff bedarf, siehe hierzu bei *Schwabenbauer*, Grundrechtseingriffe (Fn. 34), S. 294 f.

89 *Conrad*, Kernbereichsschutz (Fn. 20), S. 27 ff. m.w.N. Im Grunde erkennt das BVerfG diese Gefahr auch schon, vgl. BVerfGE 141, 220 (280).

90 *U. Buermeyer*, Stellungnahme zur Ausschussdrucksache 18(6)334, S. 5.

91 Instruktiv bei *Conrad*, Kernbereichsschutz (Fn. 20), S. 46 f.

2. Vorratsdatenspeicherung

Die sog. Vorratsdatenspeicherung, also die anlasslose Speicherung von Telekommunikationsverkehrsdaten[92], wurde vom BVerfG bereits von Beginn an im Lichte des Totalüberwachungsverbots betrachtet.[93] Blickt man auf die technische Möglichkeit, bereits aus Verkehrsdaten umfassende Persönlichkeitsprofile erstellen zu können, leuchtet das ein.[94] Das Totalüberwachungsverbot als Teil der verfassungsrechtlichen Identität nach Art 79 Abs. 3 GG[95] würde nicht nur einer nationalen Lösung, sondern auch einer europarechtlich determinierten Vorratsdatenspeicherung Grenzen setzen. Auch hier lassen sich Aussagen zur Verletzung aber nur im Einzelfall treffen: Da Verkehrsdaten dezentral bei den Diensteanbietern gespeichert werden[96], bedeutet erst die behördliche Zusammenführung der Daten im Falle von Ermittlungen eine Gefahr der Rundumüberwachung beziehungsweise der Bildung von Persönlichkeitsprofilen.

D. Zukunft des Totalüberwachungsverbots

Das vom BVerfG entwickelte Totalüberwachungsverbot klingt vom Namen her pathetisch und wie eine letzte Verteidigungslinie, bevor ein Rechtsstaat zum orwellschen Überwachungsstaat kippt. Die Auswertung der Rechtsprechung des BVerfG zu diesem Verbot der Rundumüberwachung hat jedoch gezeigt, dass es im Wesentlichen um die Bildung von Persönlichkeitsprofilen geht, die Menschen für den Staat vorhersehbar und prognostizierbar machen und damit den Menschen zum bloßen Objekt staatlicher Datenverarbeitung degradieren. Von dieser absoluten Grenze für staatliche Informationseingriffe der Sicherheitsbehörden liegt auch ein dystopischer Überwachungsstaat noch etwas entfernt. Die hier behandelten Beispiele von Befugnissen zur Sicherheitsgewährleistung, die sich im Rahmen der

92 § 3 Nr. 70 TKG.
93 BVerfGE 125, 260 (324).
94 *B. Perez/M. Musolesi/G. Stringhini*, You are your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information, 2018, https://arxiv.org/abs/1803.10133 (zuletzt aufgerufen am 10.10.2024); *T. Schwabenbauer*, Kommunikationsschutz durch Art. 10 GG im digitalen Zeitalter, AöR 137 (2012), 1 (9 f.).
95 BVerfGE 125, 260 (324): „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland".
96 Vgl. § 175 Abs. 1 S. 1 TKG.

Digitalisierung herausgebildet haben, zeigen die Schwächen dieser dogmatischen Figur: Sie ist weitgehend konturlos und im Einzelfall kaum operationalisierbar. Die Anwendung dieses Postulats geht in der gerichtlichen Prüfung kaum über das berühmte „I know it when I see it" hinaus.[97]

Mit einigen wenigen Maßstäben zur Gefahr von Persönlichkeitsprofilen oder einer entsprechenden verfassungsrechtlichen Definition würde sich das Totalüberwachungsverbot ganz ohne kleinteilige[98] sicherheitsverfassungsrechtliche Rechtsprechung jedoch als eine handhabbare letzte Messlatte im Sicherheitsrecht etablieren. Für die Praxis der Strafverfolgungsbehörden, Nachrichtendienste und Polizeien in Bund und Ländern bedeutet dies aber, dass das Totalüberwachungsverbot nicht Angelegenheit des Gesetzgebers ist, sondern vielmehr die eigene. Die Digitalisierung erleichtert Profilbildung enorm, weshalb das Totalüberwachungsverbot als absolute Grenze staatlicher Informationseingriffe in konkreten Ermittlungen mitgedacht werden muss. Sich allein an immer kleinteiligeren Vorgaben des BVerfG zur Vereinbarkeit sicherheitsrechtlicher Maßnahmen mit dem Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG festzuhalten ist angesichts der technischen Möglichkeiten in den Händen der Sicherheitsbehörden zu wenig.

97 U.S. Supreme Court *Jacobellis v. Ohio*, 378 U.S. 184 (1964), S. 197.

98 Zu dieser Kritik siehe nur *U. Volkmann*, Die Dogmatisierung des Verfassungsrechts, JZ 2020, 965 (969).