Brauchen wir ein Recht auf „digitalen Herdenschutz"? – Die Gefahren kommerziellen Profilings für die pluralistische Demokratie und gesellschaftliche Minderheiten

Dirk Müllmann

I. Die Funktionsweise und Gefahren von kommerziellem Profiling

„*I don't want to live in a world, where everything that I say, everything I do, everyone I talk to, every expression of creativity, or love, or friendship is recorded (…)*"[1] sagte Edward Snowden im Jahr 2013 über die Gefahr umfassender staatlicher Überwachung. Doch längst leben wir in einem technischen Umfeld ubiquitärer Datenverarbeitung, in dem nahezu jeder Vorgang in der realen Welt eine virtuelle Entsprechung findet. Der Großteil dieser Erfassung, Speicherung und Analyse unserer Daten findet jedoch nicht allein durch staatliche Stellen, sondern durch private Akteure statt, die unser Nutzungs- oder Konsumverhalten mit Hilfe von Profiling auswerten, um so ihre Produkte und Angebote zu optimieren.[2]

Das technische Vorgehen beim Profiling unterscheidet sich je nach dem Umfeld und dem Gerät, mit dem es stattfindet. Neben der Nutzung von *first-* oder *third*-party *cookies*, *Browser-* oder *Device-Fingerprints* erfolgt die Erfassung von Daten auch über das Smartphone selbst, dessen Sensoren oder auf ihm installierten Apps.[3] Auch über andere vernetzte Objekte, wie Au-

1 Ewen MacAskill, Interview: Edward Snowden, NSA files source: 'If they want to get you, in time they will', The Guardian, 10.06.2013, https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why (Stand: 12.04.2020).

2 *Christl/Spiekermann*, Networks of Control, 2016, 24; *Sehic/Rengers/Hense*, Internet of Things, in Taeger (Hrsg.), Internet der Dinge, 2015, 393 (395); *Gerhartinger* ZD 2012, 303; *Hoeren* ZD 2011, 3; *Grages*, Marketing per Datenanalyse und Zielgruppenbildung, in Taeger (Hrsg.), Law as a Service, Bd. 2, 2013, 815.

3 *Christl/Spiekermann*, Networks of Control, 2016, 45ff.; *Eckersly*, How unique is Your Web Browser, in Atallah/Hopper (Hrsg.), Privacy Enhancing Technologies, 2010, 1 (3ff.); *Mayer/Mitchell*, Third-Party web Tracking: Policy and Technology, in IEEE, Proceedings of the 2012 IEEE Symposium on Security and Privacy, 2012, 413 (415ff.); *Gabriel/Cornels*, MMR 2008, XIV (XIV f.); *Karg/Kühn* ZD 2014, 285 (286f.); *Busche/Rabus*, Customer Tracking, in Taeger (Hrsg.), Die Welt im Netz, 2011, 463 (465ff.).

tos, *Wearables*, *Smart Home* Geräte oder digitale Sprachassistenten können Anbieter eine Vielzahl sensibler Daten sammeln.[4] Dabei stehen wir erst am Anfang der umfassenden Vernetzung unseres Alltags durch das *Internet of Things*, dessen Einbindung in unser Leben, auch vor dem Hintergrund der Vision einer Industrie 4.0,[5] immer weiter zunehmen wird.[6]

Für benachteiligte und diskriminierte Gesellschaftsgruppen birgt die technische Entwicklung angesichts des Missbrauchspotentials der Mengen an sensiblen Daten bedeutende Risiken, da es wahrscheinlich erscheint, dass zukünftig auch themenfremde Daten für Prognoseentscheidungen herangezogen werden, z.B. Gesundheitsdaten bei der Kreditvergabe.[7] Die verarbeiteten Daten erlauben zudem sichere Schlüsse auf Diskriminierungsmerkmale, wie die sexuelle Orientierung, politische oder religiöse Einstellungen oder Herkunft und Ethnie.[8] Diese Angaben können angesichts ihrer umfassenden Verfügbarkeit in Kontexten herangezogen werden, in denen sie keine Rolle spielen und bisher nicht sichtbar waren. Benachteiligten Personengruppen droht vor diesem Hintergrund ein gesellschaftliches „Pariadasein", in dem sie aufgrund der umfassenden diskriminierenden Berücksichtigung einzelner Eigenschaften in sachfremden Kontexten privatwirtschaftlich von Verträgen, Netzwerken und gesellschaftlich relevanten Beteiligungsmöglichkeiten ausgeschlossen werden. Für den er-

4 *Christl/Spiekermann*, Networks of Control 2016, 52ff.; *Völkel*, Wearables und Gesundheitsdaten, in: Taeger (Hrsg.), Internet der Dinge, 2015, 35 (43); *Dregelies* VuR 2017, 256; *Kopp/Sokoll* NZA 2015, 1352; *Braun* ZD 2018, 71; *Cimiano/Herlitz* NZM 2016, 409 (412ff.); *Ametbichler* InTer 2019, 169 (170); *Schaar*, Siri, Alexa und das KI Dilemma, https://peter-schaar.de/siri-alexa-und-das-ki-dilemma (Stand: 12.04.2020); *Wagner/Eidenmüller* ZfPW 2019, 220 (224 f.).

5 *Müllmann* WRP 2018, 1177 (1178) mwN.; *ders.*, Smart Regulation for Smart Industry, in Taeger, Smart World - Smart Law?, 2016, 603 (603ff.).

6 *Christl/Spiekermann*, Networks of Control, 2016, 69ff.; *Boes/Ziegler*, Der Aufstieg des Internet of Things, 2018, 9ff.

7 Schon heute setzt der Arbeitsmarktservice Österreich einen Algorithmus zur optimalen Ressourcenallokation ein, der die Merkmale „Frau" und „alleinerziehende Mutter" negativ bewertet, vgl. *Fröhlich/Spiecker gen. Döhmann*, Können Algorithmen diskriminieren?, 26.12.2018, https://verfassungsblog.de/koennen-algorithmen-diskriminieren/ (Stand 12.04.2020).

8 *Christl/Spiekermann*, Networks of Control, 2016, 15; *Kosinski/Stillwell/Kohli et al.*, Personality and Website Choice in Contractor/Uzzi/Macy, Proceedings of the 4th Annual ACM Web Science Conference, 151 (151ff.).

forderlichen Pluralismus einer demokratischen Gesellschaft ist eine solche Entwicklung fatal[9] und erfordert Gegenmaßnahmen.

Wenn sich der Einzelne der Gefahren durch Erfassung und Auswertung seiner Daten im Rahmen von Profiling nicht durch eigenes Handeln erwehren kann, bedarf er der Hilfe der Mehrheitsgesellschaft. Die Situation ist vergleichbar mit dem aus der Medizin bekannten Institut des Herdenschutzes[10]. Der Begriff beschreibt die Widerstandsfähigkeit einer Gruppe gegenüber einem Krankheitsausbruch aufgrund der Immunität eines großen Teils der Gruppenmitglieder und der daraus resultierenden geringeren Wahrscheinlichkeit betroffener Individuen mit einem anfälligen Individuum in Kontakt zu kommen.[11] Es handelt sich somit um den indirekten Schutz, den eine Person durch andere erfährt. Übertragen aufs Profiling stellt sich die Frage, ob ein vergleichbarer rechtlicher Schutzmechanismus für durch die digitale Entwicklung potentiell gefährdete Gesellschaftsgruppen von der Mehrheitsgesellschaft gewährt, wie er etabliert und ausgestaltet werden kann.

Die Beantwortung dieser Fragen ist Gegenstand des folgenden Beitrags. Hierbei wird zur Vermeidung einer inzidenten Darstellung zunächst die sekundärrechtliche Regelung des Profiling untersucht. Sodann wird dessen verfassungsrechtliche Dimension betrachtet. Bevor in der Folge eine Auseinandersetzung mit dem Recht auf digitalen Herdenschutz selbst erfolgt, werden mögliche Alternativen in Form von Maßnahmen Betroffener und von Datenverarbeitern beleuchtet. Das Fazit bietet einen Ausblick auf die zukünftigen gesellschaftlichen Aufgaben im Zusammenhang mit der Regulierung neuer Technologien.

---

9 *Spiecker gen. Döhmann* Fragmentierungen, VVDStRL 77 (2018), 10 (37ff., 43f., 51); *Holtz-Bacha* in Gellner/von Korff (Hrsg.), Demokratie und Internet, 1998, 219 (224); *Hoffmann-Riem* AöR 142 (2017), 1 (13f.).

10 Die Begriffe Herdenschutz, Herdeneffekt und Herdenimmunität werden teilweise synonym verwendet, teilweise wird der Herdeneffekt als Folge der Herdenimmunität verstanden, vgl. hierzu: *John/Samuel*, Eur J Epidemiol 16 (2000), 601 (603); *Johnstone/Loeb*, Scand J InfectDiseases 43 (2011), 683.

11 Saunders, Dorland’s Illustrated Medical Dictionary, 28. Aufl. 1994, 812; John/*Samuel*, Eur J Epidemiol 16 (2000), 601; *Maurer*, PiuZ 37 (2008), 64 (65); *Schröder-Bäck/Martakis*, Bundesgesundheitsblatt 62 (2019), 472 (472f.).

II. Die rechtlichen Grundlagen von Profiling

Die zentrale Rechtsquelle des europäischen Datenschutzrechts ist die Datenschutz-Grundverordnung[12]. Mit ihrem Inkrafttreten hat das Datenschutzrecht eine noch weitreichendere europäische Integration erfahren.[13] Zwar war das nationale Recht bereits zuvor durch die europäische Datenschutzrichtlinie[14], die durch die DS-GVO vollständig abgelöst wurde, sowie die e-Privacy-Richtlinie[15], die neben der DS-GVO weiterhin Geltung beansprucht, europarechtlich hinterlegt; mit der seit Mai 2018 anzuwendenden Verordnung bleiben den Mitgliedsstaaten im umfassenden Anwendungsbereich der DS-GVO aber sowohl im privaten als auch öffentlichen Datenschutz nur noch die in der Verordnung in Form von Öffnungsklauseln vorgesehenen Regelungsräume für autonome Datenschutzrechtsetzung.[16]

1. Sekundärrechtliche Regelung des Profilings

Die DS-GVO adressiert erstmals explizit die Verarbeitungsform des Profilings und definiert sie in Art. 4 Nr. 4 DS-GVO. Es handelt sich dabei um jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, (...) zu analysieren oder vorherzusagen.

Angesichts des datenschutzrechtlichen Prinzips des Verbots mit Erlaubnisvorbehalt[17] bedarf es für den Einsatz von Profiling einer gesetzlichen Er-

12 Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 vom 4.5.2016, 1; in der Folge: DS-GVO.

13 *Kühling/Raab* in Kühling/Buchner (Hrsg.), 2017, Einleitung, Rn. 1; *Selmayr/Ehmann* in Ehmann/Selmayr (Hrsg.), 2017, Einleitung, Rn. 3f.

14 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, 31; in der Folge: Datenschutzrichtlinie.

15 Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 201 vom 31.07.2009, 37; in der Folge: e-Privacy-Richtlinie.

16 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 9, Rn. 1ff.

17 *Albrecht* in Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 6, Rn. 1; *Albers/Veit* in BeckOK Datenschutzrecht, 30. Ed., Stand 01.11.2019, Art. 6, Rn. 12; *Bretthauer* in Specht/Mantz (Hrsg.), Handbuch Datenschutzrecht, 2019, Teil A, Rn. 31.

laubnisgrundlage. Hierfür kommt zunächst Art. 22 DS-GVO in Betracht. Die Norm regelt jedoch nicht die Zulässigkeit des Profilings, sondern lediglich das Verfahren automatisierter Entscheidungen und die Nutzung von deren Ergebnissen.[18] Profiling wird daher von ihr nur insoweit erfasst, als es Bestandteil einer automatisierten Entscheidung ist.[19] Für den Sonderfall der Telemedien kann sich nach umstrittener Ansicht die Erlaubnis zur Bildung von pseudonymisierten Nutzerprofilen aus § 15 Abs. 3 TMG[20] ergeben, was aber angesichts einer Verdrängung der Regelung durch die DS-GVO,[21] jedenfalls aber der Entscheidung des EuGH zur Cookie-Einwilligung[22] abzulehnen ist. Art. 22 Abs. 2 lit. b) DS-GVO enthält ferner eine Öffnungsklausel, die sich jedoch ausschließlich auf Ausnahmen vom Verbot der automatisierten Entscheidung und nicht auf die Schaffung eigenständiger Erlaubnistatbestände für Profiling bezieht.[23] Daher setzt die neue Regelung zum *Scoring*, als Unterfall des Profilings,[24] in § 31 BDSG nunmehr in Absatz 1 Nr. 1 auch die Einhaltung des Datenschutzrechts explizit voraus und kann anders als zuvor noch § 28b BDSG a.F.[25] nicht als Erlaub-

18 *Buchner* in Kühling/Buchner, 2. Aufl. 2018, Art. 22, Rn. 11; *von Lewinski* in BeckOK Datenschutzrecht, 30. Ed., Stand 01.11.2019, Art. 22, Rn. 3f.

19 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 3, Rn. 6; *Kugelmann* DuD 2016, 566 (569); *Richter* ZD 2016, 581 (585); *Scholz* in Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 22, Rn. 5 mwN.

20 *Heidrich/Forgó/Moos*, Betrieblicher Datenschutz, 3. Aufl. 2019, Kapitel 1, Rn. 33; differenzierend *Jandt* ZD 2018, 405 (407ff.); ablehnend *Schmitz* in Spindler/Schmitz (Hrsg.), 2. Aufl. 2018, § 15, Rn. 87, 95ff.; *ders.* In Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 50. EL Oktober 2019, Teil 16.2, Rn. 266f.; *Kremer* in Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 28, Rn. 55, 65.

21 *Kremer* in Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 28, Rn. 55, 65; *Hullen/Roggenkamp* in Plath (Hrsg.), BDSG/DS-GVO, 3. Aufl. 2018, Einl. TMG, Rn. 13; *Jandt* ZD 2018, 405 (407).

22 EuGH, Urt. v. 01.10.2019 - C-673/17, MMR 2019 - Planet49; vgl. bereits vor dem Urteil die Widerspruchslösung bemängelnd *Schmitz* in Hoeren/Sieber/Holznagel (Hrsg.), Multimedia-Recht, 50. EL Oktober 2019, Teil 16.2, Rn. 266f.

23 *Buchner* in Kühling/Buchner, 2. Aufl. 2018, Art. 22, Rn. 48; *von Lewinski* in BeckOK Datenschutzrecht, 30. Ed. Stand 01.11.2019, Art. 22, Rn. 62f.

24 *Buchner* in Kühling/Buchner, 2. Aufl. 2018, Art. 22, Rn. 22; *Hladjk* in Ehmann/Selmayr, 2. Aufl. 2018, Art. 22, Rn. 7; *Scholz* in Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 22, Rn. 24.

25 *Lapp* in Gola/Heckmann, 13. Aufl. 2019, § 31 BDSG, Rn. 9; *Helfrich* in Forgó/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz, 3. Aufl. 2019 Kapitel 3, Rn. 25.

nistatbestand herangezogen werden.[26] Für die rechtmäßige Durchführung von Profiling muss somit auf die allgemeinen Erlaubnistatbestände in Art. 6 Abs. 1 DS-GVO zurückgegriffen werden, wobei neben einer Einwilligung nach lit. a) regelmäßig nur die Vornahme von Profiling zur Wahrung berechtigter Interessen des Verantwortlichen nach lit. f) in Betracht kommt.[27] Bei dem wohl häufigsten Fall der Durchführung von Profiling aufgrund einer Einwilligung muss diese nicht nur den in Art. 4 Nr. 11 DS-GVO niedergelegten definitorischen Anforderungen entsprechen, also freiwillig, auf einen bestimmten Fall bezogen, informiert und unmissverständlich erfolgen, sondern auch den Bedingungen des Art. 7 DS-GVO genügen.

2. *Verfassungsrechtliche Dimension des Profilings*

Angesichts der Regelung des Art. 51 Abs. 1 S. 1 EUGrCh[28] und vor dem Hintergrund der umfassenden europarechtlichen Harmonisierung des Datenschutzrechts in Form einer Verordnung scheint der heranzuziehende Grundrechtsmaßstab eindeutig aus der Europäischen Grundrechtecharta hervorzugehen.[29] Mit seinen Urteilen *„Recht auf Vergessen I und II"*[30] hat das Bundesverfassungsgericht jedoch jüngst das komplexe Wechselspiel zwischen den nationalen und europäischen Grundrechtsregimen am Beispiel des Datenschutzrechts herausgearbeitet. Vor diesem Hintergrund muss die Frage der einschlägigen Grundrechtsquelle und der aus ihr zu entnehmenden Grundrechte genauer betrachtet werden.

---

26 *Buchner* in Kühling/Buchner, 2. Aufl. 2018, § 31 BDSG, Rn. 7; *Lapp* in Gola/Heckmann, 13. Aufl. 2019, § 31 BDSG, Rn. 9; *Taeger* in Taeger/Gabler, 3. Aufl. 2019, § 31 BDSG, Rn. 56.

27 *Kremer* in Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 28, Rn. 65; *Schantz* in Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 6 Abs. 1, Rn. 121.

28 Charta der Grundrechte der Europäischen Union (2010/C 83/02), ABl. C 326 vom 26.10.2012, 391, in der Folge: EUGrCh.

29 Vgl. EuGH, Urt. v. 08.11.2016 - C-243/15, ZUR 2017, 86 (89) - Slowakischer Braunbär II; Urt. v. 14.06.2017 - C-685/15, GRUR-Int 2017, 769 (771) - Online Games; *Bieber/Epiney/Haag*, Die Europäische Union, 9. Aufl. 2011, 60, 62; *Schwerdtfeger* in Meyer/Hölscheidt, 5. Aufl. 2019, Art. 51, Rn. 40 mwN; *Nusser*, Die Bindung der Mitgliedsstaaten an die Unionsgrundrechte, 2011, 10ff.

30 BVerfG, Urt. v. 06.11.2019 - 1 BvR 16/13, NJW 2020, 300 - Recht auf Vergessen I; Urt. v. 06.11.2019 - 1 BvR 276/17, EuZW 2019, 1035 - Recht auf Vergessen II.

a) Einschlägige Grundrechtsquelle

In der Sache *Recht auf Vergessen I*[31] führt das Gericht aus, dass ein Anwendungsbereich für die Grundrechte des Grundgesetzes auch dort verbleiben kann, wo innerstaatliches Recht im Anwendungsbereich des Unionsrechts liegt, aber nicht vollständig durch Unionsrecht bestimmt wird.[32] Der Umfang der Vereinheitlichung wird dabei durch das europäische Fachrecht vorgegeben.[33] Sofern der europäische Gesetzgeber den Mitgliedsstaaten Gestaltungsspielräume in der Durchführung des Unionsrechts belässt, kann die primäre Anwendung der grundgesetzlichen Grundrechte auf den Gedanken gestützt werden, dass regelmäßig kein einheitlicher Grundrechtsschutz auf europäischer Ebene beabsichtigt ist und durch die Anwendung deutscher Grundrechte ein Vielfalt akzeptierendes, grundrechtliches Schutzniveau gewährleistet wird.[34] Von diesem alleinigen Geltungsanspruch der deutschen Grundrechte sind in Einzelfällen Ausnahmen zu machen.[35]

Gemäß der Entscheidung *Recht auf Vergessen II*[36] geht auch das Verfassungsgericht von einer vollständigen Vereinheitlichung des Datenschutzrechts aus und sieht allein die Unionsgrundrechte als einschlägig an.[37] Es betont aber, dass trotz der europäischen Rechtsvereinheitlichung einer Materie durch eine Verordnung ein mitgliedsstaatlicher Gestaltungsspielraum in Form von Öffnungsklauseln eingeräumt sein kann,[38] der als Einfallstor für die nationalen Grundrechte dient. Die Existenz einer Öffnungsklausel allein rechtfertigt jedoch noch nicht die Annahme der Gestaltungsoffenheit, da sie den Gestaltungsspielraum nur in einem bestimmten Umfang

31 BVerfG, Urt. v. 06.11.2019 - 1 BvR 16/13, NJW 2020, 300 - Recht auf Vergessen I.
32 BVerfG, Urt. v. 06.11.2019 - 1 BvR 16/13, NJW 2020, 300 (301), Rn. 42 - Recht auf Vergessen I.
33 BVerfG, Urt. v. 06.11.2019 - 1 BvR 16/13, NJW 2020, 300 (302 f.), Rn. 51, 53ff. - Recht auf Vergessen I.
34 BVerfG, Urt. v. 06.11.2019 - 1 BvR 16/13, NJW 2020, 300 (302 f.), Rn. 49, 55ff. - Recht auf Vergessen I.
35 BVerfG, Urt. v. 06.11.2019 - 1 BvR 16/13, NJW 2020, 300 (304), Rn. 63ff. - Recht auf Vergessen I.
36 BVerfG, Urt. v. 06.11.2019 -1 BvR 276/17, EuZW 2019, 1035 - Recht auf Vergessen II.
37 BVerfG, Urt. v. 06.11.2019 - 1 BvR 276/17, EuZW 2019, 1035 (1036), Rn. 32, 35 - Recht auf Vergessen II.
38 BVerfG, Urt. v. 06.11.2019 - 1 BvR 16/13, NJW 2020, 300 (305), Rn. 74 - Recht auf Vergessen I; BVerfG, Urt. v. 06.11.2019 - 1 BvR 276/17, EuZW 2019, 1035 (1037), Rn. 41 - Recht auf Vergessen II.

einräumen.[39] Gestaltungsoffenheit ist vielmehr anhand der im konkreten Fall anzuwendenden Vorschriften, nicht aber aufgrund einer generellen Betrachtung des Regelungsbereichs zu bestimmen.[40] Von einer vollständig einheitlichen Regelung kann nur ausgegangen werden, wenn ein Sachverhalt durch einen Rechtsakt auch tatsächlich abschließend geregelt werden soll.[41]

Wie zuvor bereits herausgearbeitet, ergibt sich die rechtliche Zulässigkeit der Durchführung von Profiling ausschließlich aus Art. 6 DS-GVO. Die im Zusammenhang mit Profiling existierende Öffnungsklausel in Art. 22 Abs. 2 lit. b) DS-GVO betrifft nur Ausnahmen vom Verbot der automatisierten Entscheidung und tangiert nicht die Frage der Rechtmäßigkeit des Profilings selbst. Auch wenn somit Teilaspekte des Themenbereichs Profiling mitgliedsstaatlicher Gestaltung offenstehen, ist in Anbetracht des Regelungsrahmens in der DS-GVO davon auszugehen, dass der europäische Gesetzgeber mit der Verordnung die Frage der Rechtmäßigkeit des Profilings abschließend regeln wollte. Auf sie ist daher der Grundrechtsmaßstab der EUGrCh anzuwenden.

b) Einschlägige Grundrechte

Als im vorliegenden Fall einschlägige und gegeneinander abzuwägende Grundrechte stellen sich daher Art. 8 und 16 EUGrCh dar. Art. 8 EuGrCh gewährt den umfassenden Schutz in Bezug auf die Verarbeitung aller personenbezogenen Daten unabhängig von deren Qualität oder Verarbeitungskontext.[42] Kern des Grundrechts ist seine Funktion als Abwehrrecht, die sich in der grundsätzlichen Herrschaft eines jeden über die ihn betreffenden Daten, sowie dem Schutz der freien Entscheidung äußert, ob und wofür diese Daten verwendet werden.[43] Dem Grundrecht wohnt angesichts der verankerten Auskunfts- und Berichtigungsrechte aber ebenso

39 BVerfG, Urt. v. 06.11.2019 - 1 BvR 276/17, EuZW 2019, 1035 (1041), Rn. 78f. - Recht auf Vergessen II.

40 Ebd.

41 Ebd.

42 *Bernsdorff* in Meyer/Hölscheidt, 5. Aufl. 2019, Art. 8, Rn. 20, 22; *Rengeling/Szczekalla*, Grundrechte in der Europäischen Union, 2004, Rn. 681; *Frenz*, Handbuch Europarecht, Bd. IV, 2009, Rn. 1380f.; *Bretthauer* in Specht/Mantz (Hrsg.), Handbuch Datenschutzrecht, 2019, Teil A, Rn. 13.

43 *Kingreen* in Calliess/Ruffert, Art. 8 GRC, 4. Aufl. 2011, Rn. 12; *Bock/Engeler* DVBl 2016, 593 (596); *Streinz*, Art. 8 GRC, 2. Aufl. 2012, Rn. 8; *Gersdorf* in Gersdorf/Paal, 26. Ed. 2019, Art. 8 GRC, Rn. 12.

eine Leistungs- sowie, vor dem Hintergrund der Manifestation einer Kontrollinstanz, eine organisatorische Funktion inne.[44]

Da kommerzielles Profiling durch Unternehmen und nicht von staatlichen Stellen durchgeführt wird, ist im vorliegenden Fall neben der Schutzfunktion[45] des Grundrechts insbesondere die Frage relevant, ob ihm eine mittel- oder gar unmittelbare Drittwirkung zu entnehmen ist[46]. Ein Kernargument der Drittwirkungsbefürworter stellt dabei das besondere Schutzbedürfnis von Bürgern angesichts der allgegenwärtigen Datenverarbeitung durch Konzerne dar.[47] Ebenso legen einige vom EuGH gewählte Formulierungen[48] die Annahme einer unmittelbaren Drittwirkung von Art. 8 EUGrCh nahe.[49] Sie ist aber aus dogmatischen Gründen abzulehnen. Private sind in erster Linie Grundrechtsberechtigte, nicht aber -verpflichtete.[50] Zudem sieht auch Art. 51 Abs. 1 S. 1 EUGrCh nur die Mitgliedsstaaten, Organe, Einrichtungen und sonstige Stellen der Union als durch die EUGrCh gebunden an. Eine unmittelbare Drittwirkung ist in der Rechtsprechung des EuGH ferner nur im Kontext mit Gleichheits- nicht aber mit Freiheitsgrundrechten postuliert worden.[51] Auch bedarf es der mit der Annahme einer unmittelbaren Drittwirkung verbundenen dogmatischen Verwerfungen nicht. Das Ziel des Schutzes Betroffener vor Gefahren der Datenverarbeitung durch Private kann über die Wahrnehmung der anerkannten, wenn auch nicht näher spezifizierten, Schutzdimension des Grundrechts erreicht werden und Art. 8 EUGrCh zusätzlich bei der Auslegung des Sekundärrechts eine mittelbare Drittwirkung entfalten.[52]

---

44 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 227ff., 237ff.

45 *Gersdorf* in Gersdorf/Paal, Art. 8 GRC, 26. Ed., 2019, Rn. 12; *Heselhaus/Nowak/Mehde*, Handbuch der EU-Grundrechte, 2006, § 21, Rn. 11; *Frenz*, Handbuch Europarecht, Bd. IV, 2009, Rn. 1386ff.

46 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 247ff.

47 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 247; *Spiecker* CMLR 52 (2015), 1033 (1033ff.); *Simitis* NJW 1984, 398 (401); *Rengeling/Szczekalla*, Grundrechte in der Europäischen Union, 2004, Rn. 684.

48 EuGH, Urt. v. 13.05.2014 - C 131/12, GRUR 2014, 895 (900f.), Rn. 80f., 87 - Google Spain, das von einem zu rechtfertigenden Eingriff Googles in Grundrechte spricht.

49 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 254; *Wolff* BayVBl 2015, 9 (15); *Boehme-Neßler* NVwZ 2014, 825 (828); *Danwitz* DuD 2015, 581 (584).

50 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 248f.

51 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 249; *Vilotti* ZÖR 71 (2016), 241 (246ff.).

52 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 249f.; *Streinz/Michl* EuZW 2011, 384 (387); *Jarass*, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 8,

Aus dem Grundrecht folgt somit das grundsätzliche Recht von Datenobjekten, dass sie betreffende personenbezogene Daten nicht Gegenstand einer Datenverarbeitung sind, was sich auch in Art. 6 Abs. 1 DS-GVO und dem Verbot mit Erlaubnisvorbehalt widerspiegelt. Zugleich gehört zur Herrschaft über die eigenen Daten aber auch das Recht, eine Verarbeitung zulassen zu dürfen, mithin die Anerkennung einer positiven und berechtigenden Grundrechtsdimension, die sich unter anderem in den umfassenden Verarbeitungsmöglichkeiten aufgrund einer Einwilligung zeigen (vgl. nur Art. 6 Abs. 1 S. 1 lit. a), 9 Abs. 2 lit. a), 22 Abs. 2 lit. c) DS-GVO). Sowohl ein potentiell zu schaffendes Recht auf digitalen Herdenschutz als auch zu diskutierende Ersatzmaßnahmen können daher auf eine aus Art. 8 EUGrCh herzuleitende gesetzgeberische Schutzpflicht oder aber eine mittelbare Drittwirkung gestützt werden.

Soweit es zudem aufgrund einer Datenverarbeitung zu einer Ungleichbehandlung oder Diskriminierung Betroffener kommt, ist ferner Art. 21 EUGrCh zu beachten. Er verbietet die Diskriminierung aufgrund einer Vielzahl, nicht abschließend aufgeführter Merkmale. Anders als bei Art. 8 EUGrCh wird der Norm keine unmittelbare Drittwirkung zugesprochen.[53] Im Verhältnis zwischen Privaten kommt dem Grundrecht nur im Rahmen der Auslegung des Sekundärrechts und in Form der inhaltlich übereinstimmenden Richtlinien Bedeutung zu.[54] Gegen Art. 21 EUGrCH verstoßende Normen sind zudem unanwendbar.[55] Auf die sich im vorliegenden Fall stellenden Fragen eines Rechts auf digitalen Herdenschutz zum Schutz vor Maßnahmen privater Datenverarbeiter kann die Norm da-

---

Rn. 3; *Bretthauer* in Specht/Mantz (Hrsg.), Handbuch Datenschutzrecht, 2019 Teil A, Rn. 63; BVerfG, Urt. v. 06.11.2019 - 1 BvR 276/17, EuZW 2019, 1035 (1043), Rn. 97 - Recht auf Vergessen II.

53 *Jarass*, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 21, Rn. 4; *Streinz* EUV AEUV, 2. Aufl. 2012, Art. 21 GRC, Rn. 6; *Stern* in Stern/Sachs, 2016, Art. 21, Rn. 14; *Hölscheidt* in Meyer/Hölscheidt, 5. Aufl. 2019, Art. 21, Rn. 34 mwN.

54 *Jarass*, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 21, Rn. 4; *Hölscheidt* in Meyer/Hölscheidt, 5. Aufl. 2019, Art. 21, Rn. 34; *Rossi* in Calliess/Ruffert, Art. 21 GRC, 5. Aufl. 2016, Rn. 5; *Streinz*, EUV AEUV, 3. Aufl., 2018 Art. 21, Rn. 6; EuGH, Urt. v. 03.09.2014 - C-201/13, GRUR 2014, 972 (974) - Vrijheidsfonds/Vandersteen; Urt. v. 19.01.2010 - C-555/07, NZA 2010, 85 (87) - Kücükdeveci; Urt. v. 19.04.2016 - C-441/14, NZA 2016, 537.

55 *Jarass*, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 21, Rn. 4; *Hölscheidt* in Meyer/Hölscheidt, 5. Aufl. 2019, Art. 21, Rn. 34; *Rossi* in Calliess/Ruffert, Art. 21 GRC, 5. Aufl. 2016, Rn. 5; EuGH, Urt. v. 22.11.2005 - C-144/04, NJW 2005, 3695 (3698) - Mangold; Urt. v. 19.01.2010 - C-555/07, NZA 2010, 85 (88) - Kücükdeveci; Urt. v. 11.09.2018 - C-68/17, NJW 2018, 3068 (3089); Urt. v. 17.04.2018 - C-414/16, NZA 2018, 569 (573) - Egenberger.

her nicht direkt herangezogen werden. Ihre Ausprägung in den europäischen Gleichbehandlungsrichtlinien[56] und deren Umsetzungen in nationales Recht sind in Bezug auf die Unterbindung diskriminierenden Verhaltens Privater jedoch ebenso zu berücksichtigen, wie die Möglichkeit der Auslegung datenschutzrechtlicher Normen im Lichte des Art. 21 EuGrCh. Zudem kann der europäische Gesetzgeber auf der Grundlage seiner Kompetenz in Art. 19 AEUV gesetzliche Regelungen erlassen, mit denen diskriminierendes Verhalten unterbunden werden kann.[57] Angesichts des Wortlauts der Norm ist ihm dabei jedoch ein Handlungsermessen eingeräumt.[58]

Der Datenverarbeiter, der das Profiling regelmäßig im Rahmen seiner wirtschaftlichen Betätigung vornehmen wird, kann sich wiederum auf den Schutz des Art. 16 EUGrCh berufen. Die Norm schützt die unternehmerische Freiheit in allen Ausprägungen.[59] Bei dem Recht handelt es sich im Kern um ein Abwehrrecht, mit nur begrenzten schutz- und leistungsrechtlichen Dimensionen.[60] Eine direkte Anwendung zwischen Privaten scheidet somit aus. Es ist bei der Auslegung datenschutzrechtlicher Normen jedoch als Abwägungsbelang auf Seiten der Datenverarbeiter ebenso heranzuziehen, wie es als zu wahrendes Recht bei einer etwaigen Schaffung neuer datenschutzrechtlicher Instrumente zwingend berücksichtigt werden muss.

III. Alternativen zu einem Recht auf digitalen Herdenschutz

Ein Recht auf „digitalen Herdenschutz“ ist juristisch mit der ab 01. März 2020 geltenden und zuvor kontrovers diskutierten Masernimpfpflicht des § 20 Abs. 8 - 14 IfSG vergleichbar. Beide erfordern das Tätigwerden der gesellschaftlichen Mehrheit zum Schutz anderer und verpflichten dabei unbetroffene Personen zum Handeln. Die gesetzliche Verankerung einer Handlungspflicht stellt dabei jedoch auch einen Eingriff in Grundrechte

56 Vgl. hierzu *Chege* NJ 2012, 503.
57 *Mohr* in Franzen/Gallner/Oetker, 3. Aufl. 2020, Art. 19 AEUV, Rn. 1f.; *Epiney* in Calliess/Ruffert, Art. 19 AEUV, 5. Aufl. 2016, Rn. 1f.; *Grabenwater* in Grabitz/Hilf/Nettesheim, 68. EL 2019, Art. 19 AEUV, Rn. 6, 9.
58 *Grabenwater* in Grabitz/Hilf/Nettesheim, 68. EL 2019, Art. 19 AEUV, Rn. 6.
59 *Ruffert* in Calliess/Ruffert, Art. 16 AEUV, 5. Aufl. 2016, Rn. 1; *Streinz*, EUV AEUV, 3. Aufl. 2018, Art. 16, Rn. 6; *Jarass*, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 16, Rn. 7.
60 *Bernsdorff* in Meyer/Hölscheidt, 5. Aufl. 2019, Art. 16, Rn. 10 mwN.

dar. So beinhaltet das Recht auf Datenschutz auch die Freiheit, seine Daten verarbeiten zu lassen. Aus Gründen der Verhältnismäßigkeit kann ein solcher Eingriff daher nur gerechtfertigt sein, wenn keine Maßnahmen auf Seiten der Betroffenen und der Datenverarbeiter ergriffen werden können, die ein Recht auf Herdenschutz, und damit das Handeln oder Unterlassen anderer, überflüssig machen.

1. Maßnahmen auf Seiten der Betroffenen

Es kann angesichts der fortschreitenden Verknüpfung alltäglicher Aktivitäten mit dem virtuellen Raum keine Alternative für von Benachteiligung und Diskriminierung betroffene Personengruppen sein, sich potentiell gefährlicher Technologien völlig zu enthalten. Dies würde zu einer sozialen, wirtschaftlichen und politischen Isolation innerhalb der Gesellschaft führen, da viele Dienste für sie nicht mehr nutzbar und etliche alltägliche Aktivitäten nicht mehr durchführbar wären. Dennoch sollte überlegt werden, ob die Nutzung der Angebote möglicherweise auf eine Art vorgenommen werden kann, mit der Risiken minimiert bzw. ausgeschlossen werden oder ob Gefahren mit bereits existierenden oder neuen Instituten des Datenschutzrechts eingedämmt werden können. Die hier vorgenommene Untersuchung beschränkt sich dabei auf die den Betroffenen selbst zustehenden Möglichkeiten und geht nicht auf die ebenso relevanten Wirkungen externer Effekte ein.

a) Verweigern der Verarbeitungserlaubnis

Profiling ist nur auf der Basis der Erlaubnisnormen des Art. 6 Abs. 1 lit. a) oder f) DS-GVO rechtmäßig durchführbar. Anders als im Fall des Art. 6 Abs. 1 lit. f) DS-GVO, der die Vornahme zur Wahrung berechtigter Interessen ermöglicht und Betroffenen kaum Einflussmöglichkeiten lässt, könnte im Fall der Durchführung von Profiling auf der Grundlage einer Einwilligung (Art. 6 Abs. 1 lit. a) DS-GVO) deren Erteilung verweigert werden.

Diese Verweigerung hat jedoch regelmäßig zur Folge, dass der gewünschte Dienst nicht mehr genutzt werden kann und käme somit einem Ausschluss von der Technologie gleich. Problematisch ist in diesem Zusammenhang zudem, dass sich Datenverarbeiter bei der Erteilung einer Einwilligung exzessive Möglichkeiten zur Datenerfassung und -verarbei-

tung zugestehen lassen. Dies ist eigentlich durch das in Art. 7 Abs. 4 DS-GVO enthaltenen sog. Kopplungsverbot ausgeschlossen. Hierbei handelt es sich um das Verbot, die Gewährung des Zugangs zu einem Vertrag oder einer Leistung von der Erteilung einer datenschutzrechtlichen Einwilligung abhängig zu machen, die über einen für den Vertrag erforderlichen Umfang hinausgeht.[61] Insofern besteht einerseits ein Vollzugsdefizit in Bezug auf die Bekämpfung zu umfassender Erlaubniserteilungen. Andererseits erweist sich das Kopplungsverbot aber auch als inhaltlich nicht so breit anwendbar, wie es sich auf den ersten Blick präsentiert; zumal die Wertung des Betreibers, was eine notwendige Datenverarbeitung darstellt, nur schwer überprüft werden kann.[62] Außerdem genügen in vielen Fällen bereits für die Nutzung eines Dienstes erforderliche Angaben, um daraus sensible Informationen über den Verwender abzuleiten.

Die Einwilligung stellt zudem keine so hohe praktische Zugangsschranke zur Erlangung einer Verarbeitungsgrundlage dar, wie man erwarten könnte. An ihr zeigen sich vielmehr praktische Defizite des Datenschutzrechts, die auch im Zuge der Reform und Stärkung der Anforderungen der Einwilligung nicht behoben werden konnten. Laut Art. 4 Nr. 11 DS-GVO muss es sich bei der Einwilligung zwar um eine für den bestimmten Fall, unmissverständlich und insbesondere auch freiwillige und informierte Willensbekundung handeln, Studien zeigen jedoch, dass die Nutzer weder wissen, worin sie einwilligen, noch, dass die Einwilligung in den meisten Fällen freiwillig erfolgt.[63] Es ist unmöglich die Vielzahl der Einwilligungserklärungen und deren enormen Umfang in der Einwilligungssituation zu lesen, geschweige denn zu verstehen. Die Nutzer willigen daher oftmals automatisch ein, wenn es von ihnen verlangt wird.[64] Aus diesem Grund stellt sich die Erteilung der datenschutzrechtlichen Einwilligung als „*Manzipation der Neuzeit*" dar, also als eine Handlung, deren eigentliche

---

61 *Engeler* ZD 2018, 55; *Golland* MMR 2018, 130; *Krohm/Müller-Peltzer* ZD 2017, 551 (551f.).

62 *Engler* ZD 2018, 55 (58f.); *Golland* MMR 2018, 130 (131); *Krohm/Müller-Peltzer* ZD 2017, 551 (551f.); *Schulz* in Gola, 2. Aufl. 2018, Art. 7, Rn. 26.

63 *Schermer/Custers/van der Hof* Ethics Info Technol 16 (2014), 171; *Custers/ van der Hof/Schermer et al.* scripted 10 (2013), 435; *Brockdorff/Appleby-Arnold/Montalto/Camilleri* European Citizens and Online Privacy: Towards a new Typology, 2015, https://www.researchgate.net/publication/268800126_European_Citizens_and_Online_Privacy_Towards_a_new_typology (Stand 12.04.2020); *Utz/Schaub/Degeling/Holz/Fahl* (Un)informed consent in 2019 ACM SIGSACConference on Computer and Communications, 2019.

64 Vgl. nur *Schermer/Custers/van der Hof* Ethics Info Technol 16 (2014), 171.

rechtliche Bedeutung immer mehr verloren gegangen ist.[65] Es ist daher dringend erforderlich, das Konzept der Einwilligung zu überarbeiten und realitätsnah neu zu denken, um so die Informiertheit und Freiwilligkeit der Erteilung wieder zu beleben. Konzepte hierfür sind, z.B. in Form der Information durch Piktogramme in Art. 12 Abs. 8 DS-GVO, bereits in der DS-GVO enthalten. Auch die Stärkung der Rolle der Aufsichtsbehörden mit der DS-GVO scheint geeignet, bestehende Vollzugsdefizite in Bezug auf unrechtmäßige Einwilligungserklärungen zu beseitigen.[66] Andere Ansätze, wie z.B. die Schaffung von Einwilligungsagenten,[67] müssen durch die Intensivierung interdisziplinärer Forschung noch weiter ausgereift werden.

Selbst wenn die Aussagekraft der Einwilligung auf die genannten Weisen gestärkt und die Möglichkeit zur Wahrnehmung größerer Eigenverantwortung Betroffener geschaffen werden, bleiben Fälle, in denen die Verarbeitung von Daten im Zuge des Profilings zulässig wäre (Art. 6 Abs. 1 lit. f) DS-GVO). Abgesehen von den beschriebenen praktischen Defiziten ist eine Lösung über die Verweigerung einer Einwilligung nicht praktikabel.

b) Verweigerung von Angaben

Ein weiterer Ansatz zum Selbstschutz Betroffener könnte in der Verweigerung von Angaben bestehen, die Rückschlüsse auf ein zur Benachteiligung oder Diskriminierung geeignetes Merkmal zulassen. Hierbei darf aber nicht übersehen werden, dass auch einer Nichtangabe ein Informationsgehalt entnommen werden kann. Sofern eine Person sich anders als alle anderen einer Vergleichsgruppe nicht zu einer Frage äußert, besteht darin eine Auffälligkeit, die vom Datenverarbeiter interpretiert werden kann. So kann erst recht offenbart werden, was mit der Nichtangabe eigentlich versteckt werden soll.

Es kommt hinzu, dass sich die für Profiling verwendeten Daten nur in geringem Umfang aus von Nutzern direkt gemachten Angaben zusam-

---

65 *Kamantauskas* Teises apzvalga Law review 12 (2015), 51 (78f.).

66 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 7, Rn. 2.

67 Vgl. *Matzutt/Müllmann/Zeissig et al.* myneData: Towards a Trusted and User-controlled Ecosystem for Sharing Personal Data in Eibl/Gaedke, INFORMATIK 2017, Lecture Notes in Informatics, 2017, 1073.

mensetzen. Eine Vielzahl sensibler Eigenschaften wird vielmehr mit hoher Treffsicherheit aus der Beobachtung unseres Surfverhaltens abgeleitet.[68]

Es bestünde zwar die Möglichkeit, den Zugriff auf Daten mittels technischer Anwendungen zu unterbinden.[69] Je nach Anwendungsfeld sieht sich eine solche Maßnahme jedoch Problemen ausgesetzt. So müsste ein Unterbinden der Datenerfassung meist in der Sphäre des Datenverarbeiters erfolgen, was einen Eingriff in dessen IT-Infrastruktur von außen erfordern würde, der straf- und zivilrechtlich relevant und angesichts seiner Massivität nicht per se durch die potentielle oder gar abstrakte Gefahr für Betroffene zu rechtfertigen wäre.[70] Unproblematisch ist hingegen die oft geäußerte Befürchtung, dass in diesen Fällen die Daten als Gegenleistung für die Nutzung eines ansonsten kostenlosen Angebots entzogen würden, da in diesen Austauschverhältnissen nicht die Abgabe von Daten, sondern lediglich die Gewährung einer Verarbeitungsmöglichkeit geschuldet ist.[71]

Betroffene sollten daher zwar versuchen, Angaben zu verweigern, als adäquate Maßnahme zur Erreichung eines angemessenen Schutzniveaus kann dieses Vorgehen jedoch nicht pauschal gewertet werden.

c) Recht auf Löschung

Die DS-GVO räumt den Nutzern in den Art. 12 - 23 DS-GVO gegenüber Datenverarbeitern umfassende Rechte ein. Im vorliegenden Kontext könnte das in Art. 17 Abs. 1 DS-GVO enthaltene Recht auf Löschung Bedeutung entfalten. Es gewährt den Betroffenen die Möglichkeit, die Löschung sie betreffender personenbezogenen Daten zu verlangen, wenn z.B. die Daten für den Erhebungszweck nicht mehr erforderlich sind (lit. a), die Einwilligung widerrufen wird und keine alternative Verarbeitungsgrundlage

---

68 *Christl/Spiekermann*, Networks of Control, 2016, 15, 45; *Valentino-DeVries*, What they know about you, Wall Street Journal, 31.07.2010, https://www.wsj.com/artcles/SB10001424052748703999304575399041849931612 (Stand 12.04.2020); *Kosinski/Stillwell/Kohli et al.*, Personality and Website Choice in Contractor/Uzzi/Macy, Proceedings of the 4th Annual ACM Web Science Conference, 151 (151ff.).

69 Vgl. *Wagner*, Datenökonomie und Selbstdatenschutz, im Erscheinen, 2020, Rn. 366ff.

70 Die Konsequenzen hängen von der konkreten Vorgehensweise ab, was eine generalisierende juristische Betrachtung verbietet. In Abhängigkeit vom Einzelfall wären bei einem Eingriff jedoch die Einschlägigkeit der §§ 202a - 204 sowie §§ 303a f. StGB sowie Ansprüche aus vertraglicher und deliktischer Haftung zu prüfen.

71 *Wagner*, Datenökonomie und Selbstdatenschutz, im Erscheinen, 2020, Rn. 341ff.

zur Verfügung steht (lit. b), Widerspruch gem. Art. 21 Abs. 1, 2 DS-GVO gegen die Verarbeitung eingelegt wird (lit. c) oder die Daten unrechtmäßig verarbeitet wurden (lit. d). Der Löschungsanspruch kann nicht durchgesetzt werden, sofern einer der in Art. 17 Abs. 3 DS-GVO genannten Gründe vorliegt. Abgesehen von den wenigen Konstellationen im Zusammenhang mit Profiling, in denen entweder kein Löschungsgrund vorliegt oder aber eine Ausnahme nach Art. 17 Abs. 3 DS-GVO einschlägig ist, wäre es den Betroffenen somit möglich, eine Datenverarbeitung durch Löschung der sie betreffenden Daten zu unterbinden, da sich der Anspruch im Zusammenhang mit Profiling sowohl auf die In- als auch die Output-Daten bezieht[72].

Doch auch dieser Ansatz begegnet in der Praxis erheblichen Problemen. So ist es angesichts der Vielzahl der Anbieter, an die Löschungsverlangen gerichtet werden müssten, praktisch unmöglich eine umfassende Löschung zu erreichen. Schon die Geltendmachung der Löschung gegenüber jedem Betreiber einer besuchten Webseite wäre herausfordernd, erst recht jedoch das Verlangen gegenüber allen Anbietern von *third-party-Cookies*. Dass die Niederlassungen von Anbietern zudem oftmals im außereuropäischen Ausland liegen, berührt zwar nicht deren gemäß Art. 3 Abs. 2 lit. a) DS-GVO bestehenden Verpflichtung nach dem Marktortprinzip die Regelungen der DS-GVO einzuhalten,[73] erschwert die Durchsetzung dieses Rechts jedoch enorm. Vor diesem Hintergrund scheidet daher auch das Recht auf Löschung als Ersatz für ein Recht auf Herdenschutz aus.

d) Recht zur Lüge

Aus dem Arbeitsrecht ist das Recht eines Bewerbers bekannt, unzulässige Fragen nicht wahrheitsgemäß beantworten zu müssen.[74] Eine Frage wird demnach nur als zulässig angesehen, wenn ein Arbeitgeber ein berechtigtes, billigens- und schützenswertes Interesse an ihrer Beantwortung in Hin-

72 *Kamann/Braun* in Ehmann/Selmayr, 2. Aufl. 2019, Art. 17, Rn, 36.

73 *Hornung* in Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 3, Rn. 39; *Zerdick* in Ehmann/Selmayr, 2. Aufl. 2019, Art. 3, Rn, 14; *Klar* in Kühling/Buchner, 2. Aufl. 2018, Art. 3, Rn. 60ff.

74 BAG, Urt. v. 05.12.1957 - 1 AZR 594/56, NJW 1958, 516; Urt. v. 22.09.1961 - 1 AZR 241/60, NJW 1962, 74; *Preis/Bender* NZA 2005, 1321 (1321f.); *Armbrüster* in MK-BGB, 8. Aufl. 2018, § 123, Rn. 46.

blick auf das Arbeitsverhältnis hat.[75] Das ist nur dann der Fall, wenn sein Interesse so gewichtig ist, dass dahinter das Interesse des Arbeitnehmers zurückzutreten hat, seine persönlichen Lebensumstände zum Schutz seines Persönlichkeitsrechts und zur Sicherung der Unverletzlichkeit seiner Individualsphäre geheimzuhalten.[76] Würde man diese Grundsätze auf den digitalen Raum übertragen, könnten Betroffene bei Fragen, die in ihre Privatsphäre eingreifen und gleichzeitig in einem sachfremden Kontext erfolgen, bewusst eine falsche Antwort geben.

Die Idee eines „Rechts zur Lüge" im digitalen Raum als „Datennotwehr" ist vor dem Hintergrund immer umfassenderer Überwachung und immer tieferer Eingriffe in das Privatleben nicht neu.[77] Doch wie schon in Bezug auf die Möglichkeit der Verweigerung von Angaben ausgeführt, bestehen die für Profiling genutzten Daten nur zu einem geringen Teil aus expliziten Nutzerangaben, im Übrigen aber aus Beobachtungen des Nutzerverhaltens.[78] Ein möglicher technischer Eingriff zur Übermittlung falscher Daten müsste in diesen Fällen oftmals in der Verarbeitersphäre erfolgen und wäre nicht pauschal mit abstrakten Gefahren für Betroffene zu rechtfertigen.

Ein „Recht zur Lüge", d.h. bewusste Falschangaben zum Schutz der eigenen Privatsphäre, sollte möglich sein, wenn das Geheimhaltungsinteresse des Betroffenen das schutzwürdige Interesse des Verarbeiters an der Erlangung der Daten aufgrund des Rechtsverhältnisses und mit Bezug hierauf überwiegt.[79] Insoweit kann auf die aus dem Arbeitsrecht bekannten Grundsätze zurückgegriffen werden. Da dieser Schutz jedoch nur situativ gewährt werden kann, scheidet er als adäquates Schutzmittel ebenfalls aus.

2. Maßnahmen auf Seiten der Verarbeiter

Nachdem festgestellt wurde, dass auf Seiten der Betroffenen keine Maßnahmen ergriffen werden können, mit denen sich ihr Schutz vor Diskrimi-

---

75 BAG, Urt. v. 05.10.1995 - 2 AZR 923/94, NZA 1996, 371 (371f.); Urt. v. 07.06.1984, 2 AZR 270/83, NJW 1985, 645.

76 Ebd.

77 *Ronellenfitsch* DuD 2008, 110.

78 *Christl/Spiekermann*, Networks of Control, 2016, 45; *Valentino-DeVries*, What they know about you, Wall Street Journal, 31.07.2010, https://www.wsj.com/artcles/SB10001424052748703999304575399041849931612 (Stand 12.04.2020).

79 Im Ergebnis auch *Wagner*, Datenökonomie und Selbstdatenschutz, im Erscheinen, 2020, Rn. 724ff., 738ff.

nierung und Benachteiligung ausreichend sicherstellen lässt, muss untersucht werden, ob auf Seiten der Datenverarbeiter Konzepte implementiert werden könnten, die einen Diskriminierungsschutz garantieren. Auch hierbei handelt es sich im Vergleich zu Maßnahmen, die von der Gesamtbevölkerung getroffen werden müssten, um mildere und somit durch den Verhältnismäßigkeitsgrundsatz gebotene Instrumente.

a) Zeitliche Begrenzung von Datenspeicherung

Ausgehend von Art. 5 Abs. 1 lit. e) DS-GVO, der eine zeitliche Speicherbegrenzung von personenbezogenen Daten auf die Dauer der Erforderlichkeit für den Verarbeitungszweck vorsieht, könnte man Datenverarbeitern enge zeitliche Grenzen für die Speicherung von Profilingdaten setzen. Eine solche zeitliche Speicherbegrenzung wird auch vom BVerwG als potentiell eindämmende Maßnahme für Profiling verstanden.[80] In der Tat ließen sich durch die Beschränkung des Speicherzeitraums von Daten mögliche Langzeitbeobachtungen von Personen zumindest vordergründig verhindern. Da mit einer Obergrenze für den Speicher- aber keine Grenze für den Gesamtbeobachtungszeitraum einhergeht und eine solche angesichts der wiederkehrenden Nutzung von Angeboten und der damit verbundenen notwendigen Datenverarbeitung auch nicht durchsetzbar wäre, bestünde jedoch die Gefahr, dass im Profil lediglich permanent ältere Daten gegen aktuellere ausgetauscht werden. Hierdurch würden die Profile sogar aussagekräftiger in Bezug auf aktuelles Nutzerverhalten. Eine Langzeitbeobachtung mit aktuellen Daten wäre dennoch denkbar. Zudem übersieht dieser Ansatz, wie aussagekräftig Daten von Kurzzeitbeobachtungen angesichts der Gleichförmigkeit unseres Alltags sind.[81] Sofern eine Kurzzeitbeobachtung bei einer Person in einer besonderen Lebenslage vorgenommen wird, z.B. während einer Phase gesundheitlicher Probleme oder Arbeitslosigkeit, birgt die Speicherbegrenzung zudem die Gefahr der insgesamt falschen Wahrnehmung eines Menschen mit den daraus resultierenden negativen Konsequenzen.

Eine zeitliche Speicherbegrenzung ist angesichts dieser Überlegungen daher kritisch zu hinterfragen und bietet keinen ausreichenden Schutz Betroffener vor Benachteiligung oder Diskriminierung.

80 BVerwG, Beschl. v. 25.09.2019 - 6 C 12.18, K&R 2019, 819 (821).
81 *Hammer/Müllmann* K&R 2020, 103 (104).

b) Restriktion der Dateninterpretation

Ein weiterer Ansatz zum Schutz Betroffener auf Seiten der Datenverarbeiter könnte in der Auferlegung von Restriktionen bei der Interpretation von Daten bestehen. So könnte untersagt werden, eine Nichtangabe mit einem anderen Ergebnis, als dass keine Angabe gemacht wurde, zu bewerten. Ferner wäre es denkbar, die Implementierung von privatsphäreschützenden Systemen vorzuschreiben, mit denen, insbesondere Diskriminierung ermöglichende, Ergebnisse verrauscht werden. Wie schon zuvor dargestellt, handelt es sich bei den meisten für Profiling genutzten Daten jedoch nicht um aktiv von Nutzern gemachte, sondern aus ihrem Verhalten abgeleitete Informationen.[82] Die Fälle, in denen die Interpretation einer Nichtangabe als solche relevant wäre, sind in der Praxis daher gering. Zudem existieren zwar technische Methoden aus dem Bereich der Forschung zur *Differential Privacy*[83] oder *k-anonimity*[84], um Datensätze zu verschleiern. Beim Profiling geht es jedoch gerade darum, dass einer konkreten Person bestimmte Eigenschaften zugeordnet werden. Dieses Ziel ist mit privatsphärewahrenden Techniken, mit denen ein Ergebnis verrauscht oder durch die Wahl einer sehr einheitlichen Vergleichsgruppe relativiert wird, unmöglich in Einklang zu bringen.

Der Verzicht auf die Aufnahme potentiell für Benachteiligungen oder Diskriminierung zu nutzender Eigenschaften in Profile würde wiederum dazu führen, dass durch das Nichtvorhandensein eines Merkmals, das in anderen Profilen regelmäßig zu finden ist, ein auffälliges Unterscheidungskriterium existieren würde, das explizit auf das Vorhandensein dieses Merkmals hinweist. Denkbar wäre insoweit nur, dass die Merkmalsangabe ebenfalls bei anderen Profilen unterlassen wird, in denen das Merkmal eigentlich unauffällig, d.h. nicht zu Benachteiligung oder Diskriminierung geeignet, ist, um so auf Seiten des Verarbeiters potentiell Betroffenen einen Herdenschutz zu gewähren. In diesem Fall müsste jedoch sichergestellt

82 *Christl/Spiekermann*, Networks of Control, 2016, 45; *Valentino-DeVries*, What they know about you, Wall Street Journal, 31.07.2010, https://www.wsj.com/artcles/SB10001424052748703999304575399041849931612 (Stand 12.04.2020).

83 *Dwork* in van Tiborg/Jajodia (Hrsg.), Encyclopedia of Cryptography and Security, 2011, 338 (338ff.); *Li* in Shen/Lin/Zhang (Hrsg.), Encyclopedia of Wireless Networks, Stand 2020, Eintrag Differential Privacy.

84 *Demiryurek/Shahabi* in Shekhar/Xiong/Zhou (Hrsg.), Encyclopedia of GIS, Stand 2017, 1097 (1097ff.); *Domingo-Ferrer* in Liu/Özsu (Hrsg.), Encyclopedia of Database Systems, Stand 2018, 2053 (2053ff.).

sein, dass auch den Profilinhabern, deren Angabe zum Schutz potentiell Betroffener gelöscht wurde, keine Nachteile aus deren Fehlen erwächst.

IV. Das Recht auf digitalen Herdenschutz

Die vorhergehende Untersuchung hat gezeigt, dass Maßnahmen Betroffener und Datenverarbeiter bestenfalls punktuell wirken, jedoch keinen umfassenden Schutz potentiell benachteiligter oder diskriminierter Personengruppen sicherstellen können. Insofern verbleibt ein großer Raum für Maßnahmen der Gesamtgesellschaft zum Schutz Gefährdeter.

Diese Maßnahmen stellen jedoch auch einen Selbstschutz für die freie Gesellschaft und pluralistische Demokratie dar. Demokratie bedeutet Veränderungsoffenheit.[85] Sie erfordert den begründbaren Kompromiss, der aus der Diskussion entsteht und beständig angepasst werden kann.[86] Sie birgt das Versprechen, dass aus der Position der Minderheit die der Mehrheit werden kann, da sie offen ist für Irrtümer, neue Erkenntnisse und die daraus folgenden Veränderungen.[87] In Ermangelung eines absoluten Wahrheitsanspruchs existiert in der Demokratie kein unabänderliches Allgemeinwohl, dafür aber eine Vielfalt an Konzepten und deren Pflicht einander, bei aller Auseinandersetzung, zu tolerieren.[88] Diese Dynamik der Demokratie und die Wahrung von Minderheitenrechten wird durch Profiling bedroht, das Menschen streng nach Interessen und Einstellungen trennt. Es erzeugt Teilöffentlichkeiten in Form von Echokammern und Filterblasen, die extreme Positionen fördern und angesichts ihrer Abschottung keine Auseinandersetzung mit konträren Positionen mehr erfordern.[89] Algorithmische Empfehlungen, die auf Daten zu vergangenem

85 *Spiecker gen. Döhmann* Fragmentierungen, VVDStRL 77 (2018), 10 (19); *Nolte*, Was ist Demokratie?, 2012, 283.

86 *Spiecker gen. Döhmann* Fragmentierungen, VVDStRL 77 (2018), 10 (19f.); *Schuppert* AöR 120 (1995), 32 (64).

87 *Spiecker gen. Döhmann* Fragmentierungen, VVDStRL 77 (2018), 10 (21f.); *Hesse*, Grundzüge des Verfassungsrechts, 20. Aufl. 1995, Rn. 135; *Volkmann*, Grundzüge einer Verfassungslehre, 2013, 242; *Lepsius* Der Staat 52 (2013), 157 (169).

88 *Hesse*, Grundzüge des Verfassungsrechts, 20. Aufl. 1995, Rn. 159; *Spiecker gen. Döhmann* Fragmentierungen, VVDStRL 77 (2018), 10 (22f); *Schumpeter* Capitalism, Socialism and Democracy, 1976, 295.

89 *Spiecker gen. Döhmann* Fragmentierungen, VVDStRL 77 (2018), 10 (24f., 37ff., 43, 51); *Lepsius* Der Staat 52 (2013), 157 (175f.); *Hesse*, Grundzüge des Verfassungsrechts, 20. Aufl. 1995, Rn. 135, 138; *Holtz-Bacha* in Gellner/von Korff (Hrsg.), Demokratie und Internet, 1998, 219 (224); *Ungern-Sternberg* in Unger/Ungern-Stern-

Verhalten basieren, fördern zudem die Perpetuierung bestehenden Verhaltens und somit selbsterfüllende Prophezeiungen, da nur zu bisherigem Handeln passende Optionen, nicht aber außerhalb des Interessens- und Verhaltensspektrums liegende Alternativen vorgeschlagen werden. Mit der allgegenwärtigen Datenerfassung und der Schaffung eines gläsernen Konsumenten geht zugleich ein großer Überwachungsdruck[90] einher, der Menschen dazu bewegen kann, von der Mehrheit abweichendes Verhalten zu unterlassen, um nicht aufzufallen. In China wird dieses Ziel mit der Einführung des Sozialkreditsystems sogar bewusst verfolgt.[91] Der Minderheit wird auf diese Weise die Chance genommen, zur Mehrheit zu werden und die Vielfalt der Lebensentwürfe schwindet. Profiling gefährdet so durch die Möglichkeit der Begrenzung von Zugang und Teilhabe[92] und die Katalysation des Wegfalls gesamtgesellschaftlicher Foren nicht nur Einzelne, sondern die Basis der Demokratie insgesamt und macht daher Gegenmaßnahmen erforderlich.

Die konkrete Ausgestaltung schützender Maßnahmen als Ausfluss eines Rechts auf digitalen Herdenschutz ist dabei fraglich. Es ist praktisch unmöglich, sie wie bei einer Impfung durch unkoordinierte Einzelmaßnahmen von Nichtbetroffenen sicherzustellen, da es nicht genügt, an die Bevölkerung zu appellieren, sich gelegentlich nicht mehrheitskonform und virtuell wie ein Mitglied einer gefährdeten Gruppe zu verhalten. Vielmehr bedarf es zentraler Maßnahmen durch den Gesetzgeber, der sein Tätigwerden dabei auf die aus Art. 8 EUGrCh resultierende Schutzpflicht unter besonderer Berücksichtigung der grundrechtlichen Gleichbehandlungsgebote stützen kann. Dem steht auch das Recht der Datenverarbeiter auf unternehmerische Freiheit nicht entgegen, da kein unternehmerisches Interesse eine sachgrundlose Ungleichbehandlung erfordern kann.[93]

Im Ergebnis kann ein Recht auf digitalen Herdenschutz im Zusammenhang mit Profiling daher nur die Form eines risikoadaptierten Regulierungsansatzes mit gestuften Verboten annehmen. Die Verwerfung dieser

---

berg (Hrsg.), Demokratie und künstliche Intelligenz, 2019, 3 (10), *Schumpeter* Capitalism, 1976, 263; *Hoffmann* AöR 142 (2017), 1 (13f.).

90 Vgl. hierzu nur: BVerfG, Urt. v. 02.03.2010 - 1 BvR 256/08, 263/08, 586/08, NJW 2010, 833 (838ff.); *Bretthauer*, Intelligente Videoüberwachung, 2017, 97f.

91 Vgl. nur: *Landwehr*, Digitale Überwachung: China schafft den „besseren Menschen“, 01.03.2018, becklink 2009207; *Kostka*, China’s Social Credit System and Public Opinion, 23.7.2018, https://ssrn.com/abstract=3215138 (Stand 12.04.2020).

92 *Spiecker gen. Döhmann* Fragmentierungen, VVDStRL 77 (2018), 10 (44).

93 Vgl. hierzu am Beispiel der Arbeitnehmerdiskriminierung und einer ggf. konsequenten Neutralitätsausrichtung eines Unternehmens *Schubert* in Franzen/Gallner/Oetker, 3. Aufl. 2020, Art. 16 GRCh, Rn. 38ff., 41.

in Grundzügen schon vom Europäischen Parlament im Rahmen des Gesetzgebungsprozesses der DS-GVO vorgebrachten Idee erweist sich insofern nachträglich als Fehler.[94] Es sollte je nach Kritikalität[95] des Zwecks der Datenverwendung ein Regelungssystem zur Verfügung gestellt werden, das sowohl die gesamtgesellschaftlichen Gefahren als auch die Risiken für potentiell diskriminierte und benachteiligte Gruppen minimiert. Hierbei sollte, wie bereits in § 28b BDSG a.F. in Bezug auf *Scoring* geschehen, anwendungs- oder anwendungsgruppenorientiert vorgegangen werden, um das individuelle Risikopotential der Einsatzzwecke adressieren zu können. Ein generelles Verbot der Verarbeitung von bestimmten Kategorien von Daten sollte hingegen nicht erwogen werden, da gesellschaftlich wichtige Zwecke für die grundsätzliche Verarbeitungsmöglichkeit aller Daten sprechen können, z.B. von Gesundheitsdaten zur Forschung.

In einer ersten Kritikalitätsstufe könnten Verwendungszwecke ohne großes Schädigungspotential zusammengefasst werden, wie z.B. die Verbesserung der Nutzungserfahrung einer Webseite. Für sie können die bisher existierenden Regelungen als ausreichend angesehen werden. Für Anwendungen, die bedeutendere Auswirkungen auf das Leben der Betroffenen haben, könnte in einer zweiten Kritikalitätsstufe ein Verbot der Verknüpfung konkreter Datengruppen oder der Heranziehung bestimmter Daten zu sachfremden Zwecken vorgesehen werden, wie z.B. von Gesundheitsdaten zur Kreditgewährung. In der höchsten Kritikalitätsstufe, deren Anwendungen ein inakzeptables Gefährdungspotential für Betroffene aufweisen, sollte ein Verbot der Vornahme von Profiling zu diesem Zweck stehen. Dies erscheint besonders im Bereich vieler Gesundheitsanwendungen geboten.

Diese gesetzgeberischen Maßnahmen zum digitalen Herdenschutz müssen, um effektiv wirken zu können und durchsetzbar zu sein, mit Auskunfts- und in Fällen von Verstößen auch mit Klagerechten flankiert werden. Die sich hierbei stellenden Probleme in Bezug auf die Wahrung von Geschäftsgeheimnissen der Datenverarbeiter[96] und der Nachvollziehbarkeit und Erklärbarkeit algorithmischer Entscheidungen[97] bedürfen jedoch noch weiterer rechtswissenschaftlicher Forschung und Entwicklung.

---

94 Vgl. *Scholz* in Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 22, Rn. 14.

95 *Datenethikkommission*, Gutachten der Datenethikkommission, 2019, 173ff.

96 Vgl. BGH, Urt. v. 28.01.2014 - VI ZR 156/13, NJW 2014, 1235; *Gausling* ZD 2019, 335 (340f.); *Brink/Joos* ZD 2019, 483 (483ff.); *Conrad/Schneider* in Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 11, Rn. 108.

97 *von Maltzan/Käde* CR 2020, 66 (66ff.); *Herberger* NJW 2019, 2825 (2827f.); *Hänold* ZD-aktuell 2019, 06471.

V. Fazit

„Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert oder als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. (...) Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist"[98],

stellte das BVerfG bereits 1983 mit einer beeindruckenden Weitsicht und unter Antizipation unserer technischen Gegenwart fest, als es im Volkszählungsurteil die Grundlagen des nationalen Datenschutzes legte. Es bezog sich zwar auf das Handeln des Staats selbst und nicht auf das Privater; doch wenn durch die Versagung des Zugangs zu Dienstleistungen, Netzwerken oder Verträgen eine Teilhabe am gesellschaftlichen Leben unmöglich wird, ist angesichts der Wirkungsgleichheit unerheblich, wer diesen Ausschluss herbeiführt.

Die Antwort auf die titelgebende Frage dieses Beitrags lautet daher: Wir brauchen ein Recht auf digitalen Herdenschutz. Der Staat muss sich zum Schutz des Einzelnen und der Pluralität der Demokratie derer annehmen, denen durch eine ubiquitäre Verarbeitung ihrer Daten Nachteile drohen, weil sie zu Gruppen gehören, die Ausgrenzung erfahren. Das fordert schon die Schutzdimension des Art. 8 EUGrCh. Der Herdenschutz muss jedoch nur dort greifen, wo Betroffene nicht dazu ermächtigt werden können, selbst für den eigenen Schutz einzustehen. Im Fall des Datenschutzes wäre das durch die Beseitigung datenschutzrechtlicher Vollzugsdefizite sowie die Überarbeitung von Rechtsinstituten, z.B. der Einwilligung oder des Kopplungsverbots, möglich. Erforderlich sind aber auch neue, nutzerorientierte Instrumente, wie Einwilligungsagenten, Icon-Lösungen oder Vorgaben für Mustereinwilligungserklärungen in Anlehnung an §§ 307 ff. BGB. Wo diese Mittel zur Selbstverteidigung nicht greifen, muss der Staat mit sinnvoller Gesetzgebung einspringen. Beherrschbare Gefahren können über einen Eingriff in Form techniksteuernder Regulierung eingedämmt werden. In Fällen, in denen aber angesichts unkontrollierbarer Risiken untragbare Folgen für Betroffene drohen, müssen auch Verbote ausgesprochen werden.

---

98 BVerfG, Urt. v. 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1 (43), Rn. 154 - Volkszählungsurteil.

Eine wesentliche Zukunftsaufgabe des Staates und der gesellschaftlichen Debatte wird es sein, das bereichernde Potential des digitalen Wandels gegen die mit ihm verbundenen Gefahren für das demokratische Fundament der Gesellschaft abzuwägen und ausgewogene Lösungen aufzuzeigen.