Johannes Eichenhofer

Privatheitsgefährdungen durch Private

Zur grundrechtsdogmatischen Einordnung von Internetdienstanbietern

Das Internet fordert nicht nur die Wirksamkeit zahlreicher Datenschutzbestimmungen, sondern auch unser konventionelles Verständnis von „Privatheit“ heraus. Der Beitrag schlägt deshalb ein Verständnis von Privatheit im Internet als „e-Privacy“ vor und zeigt auf, inwieweit ein solches (Grund-) Recht gegenüber privaten Internetdienstanbietern zur Anwendung kommen kann.

1 Privatheit im Internet als „e-Privacy“

Nach einer klassischen Definition bezeichnet „Privatheit“ (engl. Privacy) das Recht des Einzelnen, darüber bestimmen zu können, welche Informationen über ihn kommuniziert werden.[1] Dieser Anspruch wird durch das Ziel und die Funktionsweise des Internet fundamental herausgefordert und in gewisser Hinsicht sogar unmöglich gemacht. Schließlich dient die Vernetzung von Rechnern gerade dem Austausch von Daten[2] und Informationen[3] und nicht ihrer Geheimhaltung.[4] Der Datentransfer zwischen Server und Client ist also keine unliebsame Begleiterscheinung, sondern Zweck und Funktionsbedingung des Netzes. „Privatheit im Internet“ kann daher nicht bedeuten, dass der Einzelne das Recht hätte, diesen *funktionsnotwendigen* Datentransfer zu verhindern. Vielmehr kann nur das Recht gemeint sein, *zusätzlichen* Datentransfer (z. B. durch Tracking) zu begrenzen bzw. darüber zu bestimmen, welche *Informationen* Dritte aus dem Datentransfer gewinnen (z. B. durch Profilbildung) und an wen sie diese Informationen kommunizieren[5] dürfen. Die Informationsgewinnung ist umso leichter, je mehr Daten ein Nutzer über sich (oder einen Dritten) preisgibt und je größer der Informationswert ist, den diese Daten besitzen. In der Regel dürfte die Bereitschaft des Nutzers zur Preisgabe personenbezogener Daten vor allem gegenüber demjenigen bestehen, der ihm im Gegenzug eine bestimmte Gegenleistung anbietet. In den Fokus geraten daher vor allem diejenigen Internetdienstanbieter,[6] die elementare Bedürfnisse des Nutzers befriedigen und aufgrund dessen besonders oft genutzt werden. Hierzu gehören vor allem die Suchmaschinen und soziale Netzwerke, die dem Bedürfnis des Nutzers nach Information und Kommunikation gerecht werden.

Wann aber ist eine Suchanfrage oder eine Kommunikation in einem sozialen Netzwerk im juristischen Sinne als „privat“ anzusehen? Nach der „Sphärentheorie“ des BVerfG bestimmt sich die „Privatheit“ einer Information nach ihrem Inhalt[7], ihrer Bedeutung für öffentliche Zwecke[8] und danach, ob und gegenüber wem der Betroffene sie kommunizieren will.[9] Diese Abgrenzung ist insofern problematisch, als das Internet es erlaubt, auch aus „belanglosen Daten“ Informationen zu gewinnen und sich der (notwendige) Datentransfer nicht überschauen lässt (s. o.). Aus diesem Grund kann auch das Recht auf informationelle Selbstbestimmung, das die „Befugnis des Einzelnen“ schützt, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[10], die Problematik nicht angemessen erfassen.[11] Das „Computer-Grundrecht“ hat seine Funktion

1 Westin, Privacy and freedom (1968), 7: „Privacy is the claim of individuals ... to determine ... when, how, and to what extent information about them is communicated to others.“

2 Nach Vesting, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts, Band II, 2. Aufl. 2012, § 20 Rn 11 sind Daten „interpretationsfreie Zeichen oder Symbole, ... , die strikt formalisierbar ... und in schematischen Abläufen (Verfahren) beliebig reproduziert werden können.“

3 Demgegenüber beschreiben Informationen nach Kloepfer, Informationsrecht (2002), § 1 Rn 53 die Kodierung von Zeichen in Sinn (und umgekehrt). Siehe auch Jendrian/Weinmann, Gateway „Daten und Informationen“, DuD 2/2010, 108.

4 In diesem Sinne: Schaar, Datenschutz im Internet (2001), Rn 58: „Bei der Konzeption des Internet hat Vertraulichkeit kaum eine Rolle gespielt.“

5 Kommunikation stellt nach Vesting, (Fn 2) Rn 60 „als intersubjektive Bewegung von Information von einem Sender zu einem Empfänger letzterem ein Angebot bereit, aus dem er die für ihn relevanten Informationen entnimmt.“

6 Zum Begriff: § 2 Nr. 1 TMG, sowie unten (Abschnitt 2).

7 Beispiel: BVerfGE 27, 344 (351) – Scheidungsakten; E 32, 373 (379) – Krankenakten.

8 Beispiel: BVerfGE 34, 238 (245) – Verwertung einer Tonbandaufnahme zum Zwecke der Strafverfolgung.

9 Plastisch: Worms/Gusy, Verfassung und Datenschutz, DuD 2012, 92 (93): „ Was beim Einzelnen bleibt und von ihm nicht preisgegeben wird, oder werden will, ... ist privat, was er preisgibt ... öffentlich.“

10 BVerfGE 65, 1 (43) – Volkszählung.

11 Bull, Informationelle Selbstbestimmung – Vision oder Illusion, 2. Aufl. (2011).

Dr. Johannes Eichenhofer

wissenschaftlicher Mitarbeiter an der Fakultät für Rechtswissenschaft der Universität Bielefeld.

E-Mail:
johannes.eichenhofer@uni-bielefeld.de

demgegenüber primär beim Schutz gegen heimliche Infiltrationen.[12] Notwendig ist daher ein auf die Funktionsweise des Internet abgestimmtes Recht auf „e-Privacy“[13], welches die Kommunikation (1) „privater“[14] Informationen, die (2) auf Medien gespeichert, verarbeitet oder übermittelt werden, aber nicht unter der Kontrolle des Trägers der möglichen Privatheit stehen, und zugleich (3) nicht als geschützte Sphäre konstituiert und dadurch unzugänglich für Verarbeiter und Dritte wären (dazu Abschnitt 3). Das Konzept der „e-Privacy“ setzt also an dem Punkt an, an dem ein Internetnutzer die Kontrolle über die ihn betreffenden Daten bereits verloren hat.

2 Das Problem: Die ambivalente Rolle der Internetdienstanbieter

„Private“ Kommunikation ist im Internet nur unter Zuhilfenahme von Internetdienstanbietern – d. h. Network-, Access-, Service- und Content-Providern – möglich. Doch die Anbieter ermöglichen ihren Nutzern die Ausübung von „e-Privacy“ nicht nur, sie können sie auch gefährden. Einerseits können die Anbieter *zusätzliche* (s. o., Abschnitt 1) Daten gegen den Willen ihrer Nutzer erheben und hieraus Informationen gewinnen. Andererseits können die Anbieter die „e-Privacy“ ihrer Nutzer nicht ausreichend gegen Gefährdungen durch andere Nutzer (z. B. Hacking-Angriffe auf einen E-Mail-Account) schützen. Dies gilt grundsätzlich für alle Network-, Access- und Service-Provider.[15] Ein besonders großes Gefährdungspotential geht jedoch von bestimmten Service-Providern selbst aus, nämlich von Suchmaschinen und sozialen Netzwerken. Deren Interesse besteht nämlich nicht – wie bei den Network- und Access-Providern – in der Herstellung eines störungsfreien Datentransfers, sondern in einer möglichst umfassenden (zusätzlichen) Datenerhebung und einer möglichst umfassenden, hierauf aufbauenden Informationsgewinnung und Kommunikation an Dritte (z. B. Werbekunden). Dieses Geschäftsmodell soll keineswegs *in toto* verurteilt werden, da es dem Nutzer unbestreitbare Vorteile bringt und zudem durch Art. 12 und 14 GG geschützt ist.[16] Es steht jedoch in einem diametralen Gegensatz zum Recht auf „e-Privacy“, das nicht den Anbieter, sondern den Nutzer entscheiden lassen will, was mit „seinen“ personenbezogenen Daten geschieht. Dem Nutzer bleibt zwar rein theoretisch die Möglichkeit, die Dienste des betroffenen Anbieters nicht in Anspruch zu nehmen. Dann könnte er jedoch seine Bedürfnisse nach Information und Kommunikation nicht oder nicht äquivalent befriedigen. Schließlich steigt die Qualität datenbasierter Geschäftsmodelle mit der Anzahl ihrer Nutzer. Ein soziales Netzwerk ist daher umso attraktiver und eine Suchmaschine umso leistungsfähiger, je mehr Nutzer sie hat. Dieser „Netzwerkeffekt“ hat in den letzten Jahren dazu geführt, dass beispielsweise Google Anteile von über 90% auf dem Markt für Suchmaschinen hält.[17] Diese *Markt*macht erlaubt es dem Unternehmen seinen Nutzern aufgrund seiner Verhandlungsposition immer mehr Regeln aufzuerlegen, die deren „e-Privacy“ gefährden können.[18] Dies hat wiederum zur Folge, dass den mächtigen Anbietern noch mehr Daten zur Verfügung stehen, wodurch sie ihre marktbeherrschende Stellung und ihre Verhandlungsposition gegenüber den Nutzern verfestigen können. Vor diesem Hintergrund fragt sich, welche grundrechtsdogmatischen Lösungsansätze sich anbieten, um dieser Spirale aus *Markt*-, *Vertrags*- und *Daten*macht[19] zu begegnen.

3 Grundrechtsdogmatische Lösungsansätze

Auch wenn weder das Grundgesetz (GG) noch die Europäische Menschenrechtskonvention (EMRK) und die EU-Grundrechtecharta (GRCh) eine ausdrückliche Bindung Privater an das Recht auf Privatleben bzw. Datenschutz vorsehen, haben das BVerfG (Bundesverfassungsgericht), der Europäische Gerichtshof für Menschenrechte (EGMR) und der Europäische Gerichtshof (EuGH) verschiedene Lösungsansätze entwickelt, um den Grundrechten gegenüber Privaten zur Wirkung zu verhelfen. Dabei handelt es sich um die unmittelbare bzw. mittelbare Drittwirkung (3.1) und die staatlichen Schutzpflichten (3.2).

3.1. Drittwirkung

Grundrechtsbindungen Privater werden in Deutschland vor allem unter dem Stichwort der unmittelbaren bzw. mittelbaren „Drittwirkung“ diskutiert, während sich diese Rechtsfigur in der EMRK und der GRCh bislang nicht etablieren konnte.[20]

Eine *unmittelbare* Drittwirkung bzw. Grundrechtsbindung Privater ist angesichts des klaren Wortlauts von Art. 1 Abs. 3 GG jedoch nur hinsichtlich objektiver Grundrechtsdimensionen und zum Schutz der Menschenwürde (Art. 1 Abs. 1 GG) anerkannt.[21] Hiernach hätten Internetdienstanbieter die Ausnutzung ihrer *Daten*macht durch menschenunwürdige Datenverarbeitungen zu unterlassen. Ein Verstoß gegen Art. 1 Abs. 1 GG könnte sich dabei einerseits aus der Heimlichkeit der Datenverarbeitung[22] (z. B. durch Tracking) und andererseits daraus ergeben, dass der Internetnutzer zum Objekt bzw. bloßen Datum gemacht würde (z. B. Profiling).[23] Das Tracking mittels Cookies[24], wie es beispielsweise durch Google Analytics[25] praktiziert wird, würde allerdings nur gegen Art. 1 Abs. 1 GG verstoßen, wenn durch die

12 BVerfGE 120, 274 (314) – Online-Durchsuchung.

13 Ausführlich hierzu: Gusy/Eichenhofer/Schulte, e-Privacy, JöR 2016 im Erscheinen.

14 „Privatheit“ bedeutet hier, dass der Nutzer die wirksame Möglichkeit hat, *zusätzlichen* Datentransfer zu begrenzen und Informationsgewinnung so weit wie möglich zu steuern. Dabei gilt der aus der „Sphärentheorie“ bekannte Grundsatz: Was einmal öffentlich ist, kann nicht später wieder privat werden.

15 Zu dieser Unterscheidung etwa: Weidner-Braun, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung (2012), 51 ff.

16 Strittig ist, ob sich Suchmaschinen auch auf die Meinungsfreiheit (Art. 5 Abs. 1 GG) berufen können. Vgl. dazu Elixmann, Datenschutz und Suchmaschinen (2012), 79 ff.

17 Vgl. 20. Hauptgutachten der Monopolkommission (2012/13), 63 mwN.

18 Beispiele etwa bei: Weichert, Datenschutzverstoß als Geschäftsmodell – der Fall Facebook, DuD 2012, 716 (717 f.). Zu den technischen Grundlagen: Karg/Thomsen, Tracking und Analyse durch Facebook, DuD 2012, 729 ff.

19 Zum Problem der Datenmacht: von Lewinski, Die Matrix des Datenschutzes (2014), 56 ff.

20 Zu den Hintergründen sogleich, 3.2.

21 Schliesky et. al., Schutzpflichten und Drittwirkung im Internet (2014), 135 f.

22 Vgl. dazu BVerfGE 109, 279 (313) (324) – Großer Lauschangriff.

23 Vgl. für Bürger-Staat-Beziehungen: BVerfGE 27, 1 (6); 65, 1 (57); 109, 279 (323). Für eine Übertragbarkeit auf private Internetdienstanbieter: Kutscha, Grundrechtlicher Persönlichkeitsschutz bei der Nutzung des Internet, DuD 2011, 461 (462).

24 Vgl. dazu die sog. Cookie-RL 2009/136/EG.

25 Zu den Einzelheiten und zur rechtlichen Zulässigkeit: Steidle/Pordesch, Im Netz von Google. Webtracking und Datenschutz, DuD 2008, 324 (326 ff.). Siehe auch Ertel/Venzke-Caprarese, DuD 2014, 181 (182 f.).

Heimlichkeit das Unbewusste des Internetnutzers erforscht würde, um infolgedessen Daten zu erheben, zu speichern und zu erfassen, „die geeignet sind, den Grundrechtsträger seinem Gegenüber auszuliefern. Diese Gefahr besteht bei höchstpersönlichen, intimen Daten...".[26] Diese Voraussetzungen dürften beim Web-Tracking (gegenwärtig) jedoch nicht vorliegen. Auch das Profiling dürfte (derzeit) nicht gegen Art. 1 Abs. 1 GG verstoßen. Zwar ist laut Volkszählungsurteil des BVerfG die „Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen ... auch in der Anonymität statistischer Erhebungen unzulässig."[27] Anders als bei einer staatlichen Volkszählung besteht beim Profiling gegenwärtig aber nicht die Gefahr, dass die hierdurch generierte Datenmacht später gezielt gegen die Nutzer eingesetzt würde. Vielmehr dient das Profiling allein der Platzierung von Werbung. Vor diesem Hintergrund verwundert es nicht, dass § 15 Abs. 3 S. 1 TMG das Profiling „zu Zwecken der Werbung, Marktforschung und bedarfsgerechten Telemediengestaltung" in pseudonymisierter Form und mit Einwilligung des Nutzers erlaubt. Auch die Datenschutzgrund-VO (DSGVO)[28] verbietet „Profiling"[29], dem ein eigener Abschnitt gewidmet ist (Art. 19 f.), nicht generell. Der Einzelne hat jedoch nach Art. 20 Nr. 1 DSGVO das Recht, nicht einer allein auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihm gegenüber rechtliche Wirkung entfaltet oder ihn erheblich beeinträchtigt. Internetdienstanbieter können nach Art. 20 Nr. 1b S. 1 DSGVO verpflichtet sein, „geeignete Maßnahmen" zu treffen, „um die Rechte und Freiheiten der betreffenden Person zu wahren." Dem Einzelnen steht daher gemäß S. 2 ein „Recht auf persönliches Eingreifen" des Internetdienstanbieters „auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung" zu.

Eine *mittelbare* Drittwirkung bedeutet dagegen, dass die Grundrechte aufgrund ihrer objektiv-rechtlichen Funktion auch im Privatrechtsverhältnis bei der Auslegung zivilrechtlicher Normen, v. a. der Generalklauseln und sonstigen auslegungsfähigen Begriffen, zu berücksichtigen sind.[30] Diese Form der Grundrechtsbindung bietet sich an, um auf die *Vertrags*macht der Internetdienstanbieter zu reagieren. So hat das BVerfG in seiner Handelsvertreter-Entscheidung entschieden, dass das Grundrecht auf Berufsfreiheit nach Art. 12 Abs. 1 GG „gebieten (kann), dass der Gesetzgeber im Zivilrecht Vorkehrungen zum Schutz der Berufsfreiheit gegen vertragliche Beschränkungen schafft, namentlich wenn es an einem annähernden Kräftegleichgewicht der Beteiligten fehlt."[31] Zum Schutz der Vertragsfreiheit und der „e-Privacy" der Internetnutzer ist deshalb an die Bedeutung des Transparenzgebots (§ 307 Abs. 1 S. 2 BGB) bei der Verwendung Allgemeiner Geschäftsbedingungen seitens der Internetdienstanbieter zu erinnern. Denn nur bei einer ausreichenden Information des Nutzers kann die nach § 4a Abs. 1 S. 1 und 2 BDSG erforderliche Freiwilligkeit der Einwilligung in die Datenverarbeitung unterstellt werden.[32]

3.2 Schutzpflichten

Sowohl für das GG als auch für die EMRK und die GRCh ist anerkannt, dass die Grundrechte – zumindest im Falle einer von „mächtigen Privaten"[33] ausgehenden Gefährdung – eine Schutzpflicht des Staates begründen können.[34] So anerkannt dieser Grundsatz auch ist, so umstritten ist jedoch im Einzelfall, welche Grundrechte unter welchen Voraussetzungen eine Schutzpflicht nach sich ziehen und wie der Staat seine Schutzpflicht zu erfüllen hat. Als anerkannt dürfte mittlerweile gelten, dass der Staat für das Fernmeldegeheimnis (Art. 10 GG) eine Schutzpflicht hat und dieser durch eine grundrechtsfreundliche Ausgestaltung nachkommen muss.[35] Vor diesem Hintergrund ist zu Recht erwogen worden, diese Rechtsprechung auf die durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützten Facetten der „Privatheit" zu übertragen.[36] Dass dem Grunde nach auch für das „Recht auf Achtung des Privatlebens" nach Art. 8 EMRK bzw. Art. 7 GRCh eine Schutzpflicht besteht, wird nicht bestritten.[37] Allerdings haben weder der EGMR noch der EuGH bislang darüber entschieden, unter welchen Voraussetzungen die durch einen (mächtigen) Internetdienstanbieter verursachte Gefährdung eine staatliche Schutzpflicht nach sich zieht und wie sie zu erfüllen wäre. Generell räumt der *EGMR* den Vertragsstaaten hierbei einen Beurteilungsspielraum ein und beschränkt sich darauf zu überprüfen, ob die von den Staaten angeführten Gründe zur Erfüllung der Schutzpflicht „stichhaltig und ausreichend" sind.[38] Zwar ist der Beurteilungsspielraum der Vertragsstaaten umso geringer, je gravierender die Gefährdung für die Identität einer Person ist.[39] Doch selbst wenn der EGMR eine Kontrolle beansprucht, überprüft er hier lediglich die Verhältnismäßigkeit der ergriffenen Schutzmaßnahme. Der *EuGH* hat Schutzpflichten bislang zwar ausdrücklich nur für die Grundfreiheiten, aber noch nicht für die Grundrechte anerkannt.[40] Dies bedeutet jedoch nicht, dass er sie nicht in Zukunft noch anerkennen könnte. Vielmehr wäre eine Anerkennung wegen der „Gleichwertigkeitsklausel" des Art. 52 Abs. 3 GRCh geradezu geboten. Da der deutsche Gesetzgeber mit dem BDSG und dem TMG eine Reihe von Vorschriften zum Schutz der „Privatheit" gegenüber privaten Internetdienstanbietern erlassen hat, die zugleich auch die Interessen der Internetdienstanbieter angemessen berücksichtigen, stellt sich die Frage

26 Schliesky et al., aaO, 135 f.

27 BVerfGE 65, 1 (53); zuvor bereits: BVerfGE 27, 1 (6) – Mikrozensus.

28 Fassung vom 11. Juni 2015, Rats-Dok. Nr. 9398/15.

29 Nach Art. 4 Nr. 12 DSGVO wird „Profiling" definiert als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel zu analysieren und vorherzusagen."

30 Pieroth/Schlink/Kingreen/Poscher, Grundrechte. Staatsrecht II, 30. Aufl. 2014, Rn 196 ff.

31 BVerfGE 81, 242 (242) – Handelsvertreter.

32 Vgl. etwa OLG Köln, Urt. v. 17.6.2011, 6 U 8/11 = DuD 2011, 820 f.

33 Kutscha, DuD 2011, 461 (463) mwN.

34 Vgl. für das GG etwa: Calliess in: Merten/Papier, Handbuch der Grundrechte, Bd. II (2006), § 44 Rn 18 ff.; Für die EMRK: Ehlers, in: Ders. (Hrsg.), Europäische Grundrechte und Grundfreiheiten, 4. Aufl. (2014), § 2 Rn 29 ff. Hier lässt sich die Schutzpflicht bereits dadurch begründen, dass die EMRK gemäß ihres Art. 1 den Vertragsstaaten nicht nur negative Pflichten zum Unterlassen von Eingriffen, sondern auch positive Verpflichtungen auferlegt – vgl. hierzu: Dröge, Positive Verpflichtungen nach der EMRK (2003); Für die GRCh: Ehlers, in: aaO, § 15 Rn 45.

35 BVerfGE 125, 260 (327) – Vorratsdatenspeicherung.

36 Kutscha, DuD 2011, 461 (464).

37 Umstritten aber ist, ob auch zugunsten des Rechts auf Datenschutz nach Art. 8 GRCh eine Schutzpflicht besteht. Bejahend: Augsberg, in: von der Groeben / Schwarze / Hatje, EUV AEUV GRCh, 7. Aufl. 2015, Art. 8 GRCh, Art. 8 Rn 8; Ablehnend: Knecht, in: Schwarze, EU Kommentar, 3. Aufl. 2012, Art. 8 GRCh Rn 4.

38 Meyer-Ladewig, EMRK, 3. Aufl. 2011, Art. 8 Rn 118 mwN.

39 Meyer-Ladewig, aaO, Art. 8 Rn 119 mwN.

40 Vgl. Kingreen, in: Calliess/Ruffert, EUV/AEUV, 4. Aufl. 2011, Art. 51 Rn 25.

nach dem Verstoß gegen die Schutzpflicht gegenwärtig weder in Bezug auf das GG noch auf EMRK oder GRCh.

4 „e-Privacy" durch Aushandlung oder Regulierung?

Hiervon ist jedoch die Frage zu unterscheiden, ob der Staat berechtigt wäre, darüber hinausgehende Schutzmaßnahmen zu ergreifen. Fraglich ist also, ob er ein entsprechendes „Schutz*recht*" hätte und wie er dieses zweckmäßig wahrnehmen könnte. Das GG erlaubt dem Staat, zum Zwecke des Schutzes der Grundrechte des Einen in die Grundrechte des Anderen einzugreifen, wenn der Staat dabei durch Gesetz bzw. auf einer gesetzlichen Grundlage handelt und einen Ausgleich zwischen den beiden Grundrechten vornimmt.[41]

Vor allem aber fragt sich, ob der Interessenausgleich vorliegend überhaupt im Wege einer staatlichen Regulierung erfolge oder ob diese Aufgabe nicht den Nutzern und Anbietern selbst überlassen bleiben sollte. Dieses (derzeit geltende) „Modell der Privatautonomie" hat zweifelsohne den Vorteil, dass es die Grundrechte der Internetdienstanbieter respektiert und auch den Nutzern nicht generell verwehrt, selbstbestimmt bzw. „eigenverantwortlich"[42] zusätzlichen Datentransfer und Informationsgewinnung durch die Internetdienstanbieter zu begrenzen. Allerdings ist zu berücksichtigen, dass dieses Modell auch die oben (Abschnitt 2) genannte Gefährdungslage in Gestalt der „Machtspirale" hervorgebracht hat. Vor diesem Hintergrund fragt sich auch, inwiefern die von der Privatautonomie, aber auch von BDSG und TMG vorausgesetzte „Freiwilligkeit" der Einwilligung der Nutzer in die Datenverarbeitung seitens der Internetnutzer angenommen werden darf.[43] Diese Annahme kann vor allem angesichts der Intransparenz der Datenverarbeitung und den mangelnden Alternativen[44] der Nutzer mit Fug und Recht bezweifelt werden.

Demgegenüber erweist sich ein „Modell der Regulierung"[45] dann als vorteilhaft, wenn das Modell der Aushandlung und der (regulierten) Selbstregulierung[46] keinen ausreichenden Grundrechtsschutz gewährleistet und deshalb die Schutzpflicht der Grundrechte ein staatliches Eingreifen erfordern.[47] Ein solches Modell müsste keineswegs bedeuten, dass der Staat abstrakt definiert, welche Nutzerdaten er als „privat" und deshalb schutzwürdig ansieht. Denn dies liefe zweifelsohne auf eine Bevormundung[48] der Bürger hinaus und würde dem die Privatheit leitenden Prinzip der Selbstbestimmung zuwiderlaufen. Auch ist angesichts der Grundrechte der Anbieter zu berücksichtigen, dass „Privaten ... (grundsätzlich) nicht ... vorgeschrieben werden (kann), für welche Zwecke genau sie sich für welche Daten interessieren dürfen, und schon gar nicht kann jede Zweckänderung und Weiterleitung von Daten an Dritte einem Gesetzesvorbehalt unterliegen."[49] Allerdings wird für „bestimmte kommerzielle Nutzungen"[50] eine Regulierung erwogen. Eine solche – über das geltende Recht hinausgehende – Regulierung müsste dann das Ziel haben, dem Nutzer die Möglichkeit einzuräumen, *zusätzlichen* (s. o., Abschnitt 1) Datentransfer und Informationsgewinnung seitens der Internetdienstanbieter wirksam zu begrenzen. Der Nutzer muss deutlich machen können, wenn er bestimmte Informationen als „privat" und damit besonders schutzbedürftig einordnen will, wie dies z. B. gegenwärtig bei den „Privacy"-Settings von Facebook[51] möglich ist. Diese Funktion erlaubt den Facebook-Nutzern jedoch lediglich, bestimmte Informationen gegenüber anderen Facebook-Nutzern geheim zu halten und zu verhindern, dass das eigene Facebook-Profil für Außenstehende im Web angezeigt wird. Schutz gegenüber den Internetdienstanbietern gewähren diese Einstellungen nicht. Erforderlich wäre daher, die Internetdienstanbieter zum Bereitstellen weiterer Angebote zum System-[52] (z. B. Maßnahmen zur Sicherung der Nutzerdaten auf den Servern der Internetdienstanbieter, Vorabeinstellungen für opt-in-Lösungen, z. B. in Form eines ausdrücklichen Verbotes der Profilbildung von Werbeeinstellungen[53] eine externe Kontrolle, um sicherzustellen, dass der Internetdienstanbieter nicht mehr erforderliche Daten tatsächlich löscht) und Selbstdatenschutz[54] (z. B. einer End-zu-End-Verschlüsselung oder der Verwendung des SSL-Protokolls[55]) zu verpflichten. Ein wirksamer Selbstdatenschutz setzt schließlich voraus, dass Schutzmaßnahmen nicht nur auf den Endgeräten der Nutzer, sondern auch auf den Servern der Dienstanbieter eingesetzt werden.[56] Eine darüber hinausgehende Regulierung (z. B. in Gestalt einer „informationellen Entflechtung" großer Internetdienstanbieter[57]) – und sogar eine unmittelbare Grundrechtsbindung[58] – erscheint umso eher angezeigt, je mehr die Internetdienstanbieter öffentliche Aufgaben[59] wahrnehmen und hierbei „staatsähnlich" handeln.[60]

41 Vgl. etwa Jarass in: Ders., GG, 13. Aufl. 2014, Vorb. vor Art. 1 Rn 48, Art. 20 Rn 122; Ähnlich Pieroth/ Schlink/Kingreen/Poscher, aaO, Rn 91 ff. (Grundrechte als negative Kompetenznormen).

42 Vgl. Nettesheim, in: Grabenwarther (Hrsg.), Europäischer Grundrechtsschutz. Enzyklopädie Europarecht (2014), § 9 Rn 72.

43 Kritisch insoweit Wolff, Beschränkte Internettauglichkeit des BDSG, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raums (2012), 193 (196).

44 Worms/Gusy, aaO, 92 (97).

45 Skeptisch: Schliesky et al., aaO, 157: Bereits „derzeit dominiert ... ein Ansatz, der das Datenschutzrecht so einsetzt, dass es den Einzelnen vor sich selbst schützt." Kritisch auch: Augsberg, aaO, Art. 8 Rn 11: „Als Regelfall gilt ..., dass Union und Mitgliedstaaten nicht die Aufgabe haben, dem Einzelnen die materiellen Bedingungen für die Entfaltung seiner Privatsphäre zur Verfügung zu stellen."

46 Dazu etwa jüngst: Friederike Voskamp, Transnationaler Datenschutz. Globale Datenschutzstandards durch Selbstregulierung (2015).

47 Vgl. Greve, Drittwirkung des grundrechtlichen Datenschutzes im digitalen Zeitalter, in: FS Kloepfer, 665 (674 f.).

48 Kutscha, DuD 2011, 461 (464).

49 Masing, Herausforderungen des Datenschutzes, NJW 2012, 2305 (2307).

50 Masing, aaO, 2305 (2307).

51 https://www.facebook.com/help/325807937506242/.

52 Vgl. zu diesem Ansatz: Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, JZ 2014, 53 ff.

53 Dies ist erforderlich, um einer Überlastungen der Nutzer bei den Privacy-Settings entgegenzuwirken – vgl. dazu: Grimm/Bräunlich, Vertrauen und Privatheit. Anwendung des Referenzmodells für Vertrauen auf die Prinzipien des Datenschutzes, DuD 2015, 289 (291).

54 Vgl. zu diesem Konzept etwa: Forum Privatheit, White Paper Selbstdatenschutz (2014). Im Internet abrufbar unter: http://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit _White_Paper_Selbstdatenschutz_2.Auflage.pdf.

55 Secret Sockets Layer (https://).

56 Forum Privatheit, aaO, 21.

57 Dies wird etwa in Bezug auf Google diskutiert – vgl. Bundeswirtschaftsminister Gabriel in der FAZ v. 16.5.2014 – vgl. www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/sigmar-gabriel-konsequenzen-der-google-debatte-12941865.html.

58 In diese Richtung Mayer, Diskussionsbeitrag VVDStRL 74, 462 f.

59 Aufgaben sind „öffentlich", wenn sie im öffentlichen Interesse liegen – vgl. BVerfGE 15, 235 (241) – Zwangsmitgliedschaft. Ein wirksamer Schutz der Privatheit ist jedoch nicht nur im Interesse des Einzelnen, sondern der Gesellschaft insgesamt – vgl. BVerfGE 65, 1 (41) – Volkszählung.

60 Viel spricht dafür, dass etwa Google bereits gegenwärtig diese Voraussetzungen erfüllt. Immerhin sind sie seit dem „Google Spain"-Urteil des EuGH, Rs. C-131/12, Rn 77, 96 f. dafür zuständig über Anträge zu entscheiden, mit denen Nutzer ihr „Recht auf Vergessen" gelten machen wollen.

5 Fazit und Ausblick

Das Grundrecht auf „e-Privacy" ist in GG, EMRK und GRCh bereits angelegt. Während seine unmittelbare Anwendbarkeit gegenüber den Internetdienstanbietern jedoch nach gegenwärtigem Stand nicht in Betracht kommt[61], findet es seinen Niederschlag über die mittelbare Drittwirkung und die Schutzpflichten im einfachen Gesetz (BDSG, TMG, BGB) bzw. dem europäischen Sekundärrecht (v. a. Datenschutz-RL 95/46/EG, e-Privacy-RL 2002/58/EG und DSGVO). Das einfache Recht versucht bereits, auf viele Gefährdungen durch die Internetdienstanbieter zu reagieren (z. B. durch Verpflichtungen der Internetdienstanbieter zu Transparenz[62] oder Datensicherheit[63]). Eine weitergehende Regulierung ist aber umso eher notwendig, je mehr die Internetdienstanbieter in die Rolle staatlicher Akteure hineinwachsen.

Damit ist aber noch nichts über die Durchsetzbarkeit der „e-Privacy"-Regulierung gesagt. Probleme stellen sich hier vor allem aufgrund der Trans- bzw. Internationalität der Datenverarbeitung.[64] Sowohl das BDSG als auch Art. 4 Abs. 1 Datenschutz-RL 95/46 und Art. 3 DSGVO machen die Anwendbarkeit des EU-Rechts davon abhängig, dass der Internetdienstanbieter eine „Niederlassung" innerhalb der EU oder einem Drittstaat hat, in dem kraft internationalen Rechts das Recht eines EU-Mitgliedstaats gilt.[65] Allerdings hat der EuGH dieses Kriterium in seiner „Google Spain"-Entscheidung derart großzügig ausgelegt, dass auch eine Bindung der Muttergesellschaft begründet werden konnte.[66] In seinem kürzlich ergangenen „Schrems"-Urteil[67] hat der EuGH nun die Übermittlung personenbezogener Daten der europäischen Facebook-Nutzer von der irischen Facebook-Niederlassung an die Konzernmutter in den USA jedenfalls auf Grundlage der sog. „Safe Harbor"-Entscheidung[68] der EU-Kommission gestoppt. Diese habe zur Folge, dass nationale Kontrollstellen (Art. 28 RL 95/46/EG) wie z. B. der irische Datenschutzbeauftragte keine Möglichkeit gehabt hätten, gegen die Übermittlung der Nutzerdaten in die USA vorzugehen, obwohl die Kommission in ihrer Entscheidung nicht positiv festgestellt habe, dass die USA über ein „angemessenes Schutzniveau" (Art. 25 Abs. 1 RL 95/46/EG) aufweise, was aber eine Voraussetzung der Übermittlung von personenbezogenen Daten in einen Drittstaat sei. Da aber die personenbezogenen Daten in den USA nicht ausreichend gegen einen Totalzugriff seitens der US-amerikanischen Behörden gesichert seien, verletze die „Safe Harbor"-Entscheidung der Kommission den Wesensgehalt (Art. 52 Abs. 1 GRCh) des Grundrechts auf Privatleben (Art. 7 GRCh) und auf einen wirksamen Rechtsbehelf (Art. 47 GRCh). Damit ist aber eine Übermittlung personenbezogener Daten in Drittstaaten nicht gänzlich ausgeschlossen. So erlaubt etwa Art. 26 Abs. 1 lit. a) RL 95/46/EG, die Übermittlung personenbezogener Daten in einen Drittstaat von einer Einwilligung des Betroffenen abhängig zu machen. Die EU und ihre Mitgliedstaaten sind nach der „Schrems"-Entscheidung daher umso stärker verpflichtet, das gegenwärtige Datenschutzrecht daraufhin zu überprüfen, bis zu welchem Punkt sich das Aushandlungsmodell (noch) bewährt und ab wann eine (zusätzliche) Regulierung angezeigt ist. Und sie zeigt, dass Datenschutz als Konkretisierung von „e-Privacy" nur wirksam ist, wenn die mit seiner Durchsetzung beauftragten Institutionen effektive Entscheidungs- und Handlungsspielräume haben.

61 Nach Pöschl, VVDStRL 74 (2014), 405 (416) kommt die unmittelbare Drittwirkung jedoch „ins Spiel, wenn der Schutzgesetzgeber ausfällt."

62 Vgl. etwa Art. 8 RL 2002/58/EG.

63 Vgl. etwa Art. 4 RL 2002/58/EG.

64 Vgl. dazu etwa Aurelio Lopez-Tarruella, The International Dimension of Google Activities: Private International Law and the Need of Legal Certainty, in: Ders. (Hrsg.), Google and the Law (2012), 329 ff.

65 Nicht durchsetzen konnte sich dagegen der Vorschlag, die Anwendbarkeit bereits immer dann zu bejahen, wenn personenbezogene Daten von Unionsbürgern verarbeitet würden – vgl. hierzu Spindler, DJT-Gutachten (2012), F 114.

66 EuGH, aaO, Rn 48 ff. (56).

67 EuGH, Urt. v. 6.10.2015, Rs. C-362/14 – Schrems.

68 Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 (ABl. L 215, S. 7).