Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen

Ralf Poscher

Herr Slobogin kämpft in den USA für einen Verfassungsgrundsatz, den wir bereits seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahr 1983 unser Eigen nennen. Seit dem Volkszählungsurteil verfügen wir über das Grundrecht auf informationelle Selbstbestimmung, das jede staatliche Datenerhebung und Verarbeitung mit einer verfassungsrechtlichen Rechtfertigungslast verknüpft und mit detaillierten verfassungsrechtlichen Vorgaben zu Zweckbindung, Auskunfts-, Berichtigungs- und Löschungsrechten belegt. In der Perspektive eines Datenschutzbefürworters aus den USA sind wir bereits lange am Ziel der Wünsche. Wir hätten also allen Grund zufrieden zu sein.

A. Die Kritik am Recht auf informationelle Selbstbestimmung

Doch das Gegenteil ist der Fall. Nicht nur international, sondern gerade auch in der deutschen Diskussion findet sich eine stärker werdende Kritik des Rechts auf informationelle Selbstbestimmung.[1]

1 M. Albers, Zur Neukonzeption des grundrechtlichen „Daten"schutzes, in: A. Haratsch/D. Kugelmann/U. Repkewitz (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft, Stuttgart u. a. 1996, S. 113; dies., Information als neue Dimension im Recht, Rechtstheorie 33 (2002), S. 61; dies., Informationelle Selbstbestimmung, Baden-Baden 2005; dies., Umgang mit personenbezogenen Informationen und Daten, in: W. Hoffmann-Riem/E. Schmidt-Aßmann/A. Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, München 2008, § 22; W. Hoffmann-Riem, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998), S. 513; ders., Informationelle Selbstbestimmung als Grundrecht kommunikativer Entfaltung, in: H. Bäumler (Hrsg.), „Der neue Datenschutz", Neuwied 1998, S. 11; M. Kloepfer, Geben moderne Technologien und die europäische Integration Anlaß, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen? Gutachten D für den 62. Deutschen Juristentag, in: Verhandlungen des Zweiundsechzigsten Deutschen Juristentags, Bremen 1998, Bd. 1, S. 66 (81 f.); R. Pitschas, Informationelle Selbstbestimmung zwischen digitaler Ökonomie und Internet, DuD 1998, S. 139 (146); H.-H. Trute, Der Schutz personenbezogener Information in der Informationsgesellschaft, JZ 1998, S. 822 (824 ff.); ders., Verfassungsrechtliche Grundlagen, in: A. Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, S. 156 (Rn. 21 ff.); K. H. Ladeur, Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken, DuD 2000, S. 12; ders., Das Recht auf informationelle Selbstbestimmung: Eine Juristische Fehlkonstruktion?, DÖV 2009, S. 45; H. P. Bull, Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?, NJW 2006, S. 1617; ders., Informationsrecht ohne Informationskultur, RDV 2008, S. 47; ders., Informationelle Selbstbestimmung – Vision oder Illusion?: Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit, Tübingen 2009; G. Britz, Informationelle Selbstbestimmung

Im Lichte dieser Kritik stellt sich die Diskurslage in den USA und in Deutschland gar nicht so unterschiedlich dar, wie man es erwarten könnte. In beiden Rechtskreisen wird der Sinn eines allgemeinen Datenschutzrechts problematisiert – nur mit umgekehrten Vorzeichen: Während die Argumente in den USA um die Anerkennung eines Rechts auf informationelle Selbstbestimmung kreisen, richten sie sich in Deutschland auf seine Revision.

I. Das Ende der Privatheit

Die radikalste Kritik zielt nicht nur gegen das Recht auf informationelle Selbstbestimmung, sondern erklärt die gesamte Idee der Privatheit für historisch überholt. Internetautoren wie der Medienwissenschaftler Jeff Jarvis, der auch in Deutschland Säle füllt,[2] erklären bereits das „Ende der Privatheit". Privatheit erscheint ihnen als zirkuläres Konzept, als eine sich selbst erfüllende Idee, die vor den negativen Folgen schützt, die sie erst selbst hervorbringt:

Nur wenn wir Privatheit schützen, ist Privatheit schützenswert. Nur dort wo Privatheit etabliert ist, kann Öffentlichkeit beschämen. „Unter Nudisten ist niemand nackt!" lautet der Slogan. Unter den Bedingungen einer durch allgemeine Öffentlichkeit gesicherten „mutually assured humiliation"[3] werden wir – so die Prognose – auch durch unsere Fehltritte und Entgleisungen nicht mehr erpressbar sein. Anders als Bill Clinton musste Barack Obama im Wahlkampf bereits nicht mehr leugnen, inhaliert zu haben.[4] Der jugendliche Drogenkonsum ließ sich bereits nicht mehr skandalisieren, weil jeder wusste, dass der Skandal ubiquitär ist. Nichts anderes wird in Zukunft – so die Propheten des Endes der Privatheit – für kompromittierende Bilder oder Videosequenzen von Entgleisungen auf Partys, Mesalliancen, Pornographie etc. gelten. Und was sei schlecht daran, wenn die jugendlichen Fehltritte unserer Politiker demnächst öffentlich sind? Sei es nicht auch demokratischer, wenn wir ein öffentliches, transparentes Leben führen?[5]

---

zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: W. Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, Tübingen 2010, S. 561.

2 S. Vogt, Macht euch nackig!, Die Zeit v. 15.4.2010: http://www.zeit.de/digital/internet/2010-04/republica-jeff-jarvis-privat (9.11.2011).

3 J. Jarvis, http://www.buzzmachine.com/2007/11/28/friends-forever-the-advantages-of-publicness/ (9.11.2011).

4 Vgl. zu Clintons feinsinniger Einlassung den Bericht der New York Times v. 30.3.1992, „Clinton tried marijuana as a student, he says": http://www.nytimes.com/1992/03/30/news/30iht-bill_1.html (9.11.2011); zu Obama K. Seelye, Barack Obama, asked about drug history, admits he inhaled, New York Times v. 24.10.2006: http://www.nytimes.com/2006/10/24/world/americas/24iht-dems.3272493.html (9.11.2011).

5 Vgl. hierzu ausführlich J. Jarvis, Public Parts. How sharing in the Digital Age improves the way we work and live, New York 2011.

Die Gegner der Privatheit weisen zudem auf die vertanen Chancen hin, wenn wir Teile unseres Lebens der Öffentlichkeit entziehen. Nach seiner Prostatakrebsdiagnose sei sein erster Gedanke gewesen, die Diagnose und die medizinischen Details auf seinem Blog zu veröffentlichen, schreibt Jeff Jarvis. Durch die Veröffentlichung habe er Hilfsangebote, Erfahrungsberichte und Hinweise erhalten, die ihm überhaupt erst eine optimale Therapieentscheidung erlaubt hätten. Was ist die Moral der Geschichte? Der Öffentlichkeit verdankt er sein Leben oder umgekehrt: „Privacy can kill."[6]

Autoren wie Jarvis arbeiten an einer Theorie der Öffentlichkeit, die vor allem auch den wirtschaftlichen Interessen der großen Akteure des Internets in die Hände spielt. „What would Google do?"[7] lautete bezeichnenderweise das Buch, das ihn berühmt gemacht hat. Anfang 2010 legte Facebook, das weltweit größte virtuelle soziale Netzwerk, den Schalter von privat auf öffentlich um. Die Standardeinstellung der Seite wurde dahin geändert, dass alle Daten der knapp einer halben Milliarde Nutzer künftig nicht mehr privat, sondern öffentlich sein sollten. Öffentlichkeit löste Privatheit als Paradigma ab. Nur durch besondere Einstellungen sollten die Nutzer den allgemeinen Zugriff auf ihre Daten beschränken können. Auf die Forderung nach der Rücknahme dieser Änderung reagierte der Geschäftsführer, Mark Zuckerberg, mit dem Hinweis auf geänderte Privatheitskonventionen, an die sich sein Unternehmen anpassen müsse. Er habe lediglich das getan, was er getan hätte, wenn er sein Unternehmen heute gründen würde, sagte Zuckerberg.[8] Facebook wollte den Zeitgeist aufgreifen und wohl auch ein Stück vor sich her treiben. Aufgrund massiver Proteste musste die Änderung vorerst noch einmal teilweise zurückgenommen werden, neben wirtschaftlichen Interessen war es aber auch der Zeitgeist, der den Gedanken der Umstellung des Paradigmas überhaupt erst möglich machte.

Sollte es sich bei der Privatheit also tatsächlich um einen Irrtum der Geschichte handeln? In ihrem historischen Abriss der Geschichte der Privatheit erinnert Hannah Arendt daran, dass der Begriff auf das lateinische „privare" in der Bedeutung von berauben zurückgeht. In dem antiken Sinn ist der Mensch in Privatheit dessen beraubt, was ihn zum Menschen macht, der Teilhabe an der Polis.[9] Nicht schmeichelhafter ist auch die griechische Wurzel des Konzepts des „für sich seins" (idion), aus dem sich unser Begriff des Idioten ableitet.[10]

---

6 J. Jarvis, The German Privacy Paradox, http://www.buzzmachine.com/2010/02/11/the-german-privacy-paradox/ (9.11.2011); weniger dramatisch F. Manjoo, No More Privacy Paranoia. Want Web companies to stop using our personal data? Be ready to suffer the consequences, Slate v. 7.4.2011, http://www.slate.com/id/2290719/.

7 J. Jarvis, What would Google do?, New York u. a. 2009.

8 B. Johnson, „Privacy no longer a social norm, says Facebook founder", The Guardian v. 11.1.2011, http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy (9.11.2011).

9 H. Arendt, Vita activa oder vom tätigen Leben, Stuttgart 1960, S. 57 f.; vgl. auch R. Wacks, Privacy – a very short introduction, Oxford 2010, S. 32.

10 H. Arendt, Zwischen Vergangenheit und Zukunft. Übungen zum politischen Denken I, München u. a. 2000, S. 89; vgl. auch R. Wacks, Privacy (Fn. 9), S. 32.

II. Verselbstständigung des Rechts auf informationelle Selbstbestimmung

In der juristischen Literatur setzt die Kritik des Rechts auf informationelle Selbstbestimmung nicht so grundsätzlich an, wird aber zunehmend und mit zunehmender Schärfe geäußert. Marion Albers hält seine Konzeption im Volkszählungsurteil für „missglückt".[11] Karl-Heinz Ladeur titelte: „Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?"[12] Niemand geringeres als der erste Bundesdatenschutzbeauftragte, Hans Peter Bull, veröffentlichte jüngst einen Essayband mit dem Titel „Informationelle Selbstbestimmung – Vision oder Illusion"[13], wobei seine Sympathie der letzteren Alternative gilt.

Was Autoren wie Albers, Ladeur, Bull, aber auch den ehemaligen Verfassungsrichter Wolfgang Hoffmann-Riem[14] stört, ist eine zunehmend unplausibler werdende Verselbstständigung des Rechts auf informationelle Selbstbestimmung. Als lebensfremd wird eine in den Formulierungen des Volkszählungsurteils anklingende eigentumsähnliche Konzeption des Rechts auf informationelle Selbstbestimmung als Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen, kritisiert. Ein Recht der Bürger, wissen zu können „wer was wann und bei welcher Gelegenheit über sie weiß",[15] sei illusorisch, weil Informationen sich sozial nicht wie Eigentum kontrollieren ließen und wir in kaum einer sozialen Beziehung „wissen können, wer was wann und bei welcher Gelegenheit über <uns> weiß".[16] Die illusorische Anlage des Rechts habe es zu einem übersensiblen dogmatischen Instrument gemacht, das jeden Vorgang der Datenerhebung und -verarbeitung als Grundrechtseingriff erfasst – eine Vorstellung, die sich auch im Hinblick auf Prozessoren, die mehrere Millionen Datenverarbeitungsoperationen in der Sekunde vollziehen, ad absurdum führt.

11 M. Albers, Informationelle Selbstbestimmung (Fn. 1), S. 238; vgl. dies., Neukonzeption (Fn. 1), S. 119 f.; dies., Umgang (Fn. 1), Rn. 68.

12 K. H. Ladeur, Fehlkonstruktion (Fn. 1).

13 H. P. Bull, Vision oder Illusion (Fn. 1).

14 W. Hoffmann-Riem, Informationsgesellschaft (Fn. 1); ders., Grundrecht (Fn. 1).

15 BVerfGE 65, 1 (43).

16 M. Albers, Dimension (Fn. 1), S. 81: „Eine so gestaltete eigentumsanaloge Bestimmungsbefugnis hat, ernst genommen, vor allem wegen der Form und der Reichweite der damit bewirkten Determination ganz untragbare Folgen."; G. Britz, Grundsatzkritik (Fn. 1), S. 566 ff. (567): „Ein Informationsbeherrschungsrecht gewährte Unmögliches, weil sich die subjektiven Beobachtungen und Sinnkonstruktionen anderer schlicht nicht beherrschen lassen."; H. P. Bull, Sind Video-Verkehrskontrollen „unter keinem rechtlichen Aspekt vertretbar"?, NJW 2009, S. 3279 (3282): „Der Irrweg beginnt da, wo das BVerfG von der ‚Befugnis des Einzelnen' spricht, ‚grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen'"; ders., Vision oder Illusion (Fn. 1), S. 61 ff.

III. Abkehr vom Eingriffsabwehrrecht

Einige Autoren schlagen daher eine vollständige Neukonzeption des Datenschutzes vor, die sich weitgehend von einer subjektiv-rechtlichen Grundrechtsposition löst.[17] Verlangt werden eine Abkehr vom Eingriffsabwehrdenken und ein Verständnis des Datenschutzes als Risikorecht, das sich Vorsorgeregimen des Technik- und Umweltrechts annähert. Entsprechende Konzeptionen seien auch besser in der Lage, den Datenschutz systemisch zu verstehen und nicht bei einzelnen Datenverarbeitungsvorgängen anknüpfen zu lassen. Der Datenschutz soll danach in systemisch betrachteten Verwendungszusammenhängen abgearbeitet werden; statt Abwehr- sollten den Betroffenen Beteiligungsrechte eingeräumt werden; Datenschutzkommissionen sollten – ähnlich Ethikkommissionen – die Verwendungszusammenhänge beurteilen; Klagerechte sollten nicht einzelnen Grundrechtsträgern, sondern Datenschutzverbänden eingeräumt werden.[18] Das Datenschutzrecht sei in eine objektiv-rechtliche Informationsordnung einzubetten, in der es in ein Verhältnis zu Transparenzanforderungen und Informationsrechten zu setzen sei.[19] So sei es kein Zufall, dass Rumänien im internationalen Ranking des Datenschutzes den zweiten Platz belege, aber auch das höchste Korruptionsrisiko berge.[20]

Es steht also nicht allzu gut um das Recht auf informationelle Selbstbestimmung. Es befindet sich gleichsam im Belagerungszustand. Kann es dogmatisch so angelegt werden, dass es der hohen Dynamik der technischen und gesellschaftlichen Entwicklung und den geäußerten Bedenken Rechnung trägt?

B. Der Sinn des Rechts auf informationelle Selbstbestimmung

Im Zentrum der Kritik steht die Frage nach dem Sinn des Rechts auf informationelle Selbstbestimmung. Was genau soll eigentlich geschützt werden? Weder ein eigentumsähnlicher Schutz persönlicher Daten noch die Freiheit vor jeder personenbezogenen Datenerhebung und -verwertung kann ein sinnvoller Schutzgegenstand sein. Die Datenerhebung und -verwertung – besonders auch in nicht elektronischen Formen – ist viel zu ubiquitär und häufig auch zu harmlos, um als solche bereits zum Grundrechtseingriff erklärt zu werden. Darin unterscheidet sich der durch das Recht

17 M. Albers, Informationelle Selbstbestimmung (Fn. 1), S. 460 ff.; K. H. Ladeur, Abwehrrecht (Fn. 1), S. 15 ff.; ders., Fehlkonstruktion (Fn. 1), S. 54 f.; A. Scherzberg, Die öffentliche Verwaltung als informationelle Organisation, in: W. Hoffmann-Riem/E. Schmidt-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, Baden-Baden 2000, S. 195 (219 f.); die objektive Dimension betont auch W. Hoffmann-Riem, Informationsgesellschaft (Fn. 1), S. 522 ff.; ders., Grundrecht (Fn. 1), S. 13 ff.

18 K. H. Ladeur, Abwehrrecht (Fn. 1), S. 12 ff.; ders., Fehlkonstruktion (Fn. 1), S. 53 ff.

19 K. H. Ladeur, Fehlkonstruktion (Fn. 1), S. 54 f.

20 K. H. Ladeur, ebd., S. 54.

auf informationelle Selbstbestimmung gewährleistete Schutz von dem räumlich oder medial abgeschirmter „Datenquellen" wie der Wohnung oder der Brief- und Telekommunikation, die in Art. 13 und 10 GG besonders geschützt sind. Aufgrund ihrer räumlichen bzw. medialen Konkretisierung und Isolierung können diese besonderen Datenquellen vergegenständlicht und in dieser Vergegenständlichung unter Schutz gestellt werden. Auch der in der jüngsten Rechtsprechung entwickelte Schutz der Vertraulichkeit und Integrität des persönlichen Informationssystems[21] weist eine ähnliche Struktur wie Art. 13 und 10 GG auf.[22] Auch mit dem persönlichen Informationssystem werden Datenbestände, die sich von der Ubiquität sonstiger Datenquellen gegenständlich abgrenzen lassen, besonders geschützt.[23]

I. Daten und Informationen

Zur genaueren Bestimmung des Schutzzweckes der informationellen Selbstbestimmung wird in der datenschutzrechtlichen Grundlagendiskussion häufig der Unterschied zwischen Daten und Informationen starkgemacht.[24] Information ist danach der gegenüber dem Datum komplexere Begriff, der nicht nur das Datum als semantischen Sinnträger, als Zeichen, voraussetzt, sondern auch den Verwendungskontext, in dem Daten erst sinnstiftend interpretiert werden. Erst durch die kontextabhängige Interpretation der Daten werden Informationen gewonnen. Daraus wird die Konsequenz gezogen, dass neben den Daten auch der Verwendungskontext in die grundrechtliche Bewertung eingestellt werden muss. Daten generieren in unterschiedlichen Verwendungskontexten unterschiedliche Informationen. Besonders gut lässt sich dies für rechtliche Verwendungskontexte zeigen, in denen Daten mit Blick auf unterschiedliche Rechtsnormen unterschiedlicher Sinn beigelegt und damit eine jeweils unterschiedliche Information gewonnen wird. Aus den Daten des Strafregisters können etwa Informationen über die Zuverlässigkeit eines Gewerbetreibenden, die Geeignetheit eines Bewerbers für ein staatliches Amt, das Vorliegen der Voraussetzung für eine Aufenthaltserlaubnis oder die Gewährung einer Eingliederungshilfe abgeleitet werden.

Doch auch mit dem Hinweis auf den Informationsbegriff ist noch nicht gesagt, wovor das Recht auf informationelle Selbstbestimmung eigentlich schützen soll.

21 BVerfGE 120, 274.

22 B. Pieroth/B. Schlink, Grundrechte, Heidelberg 27. Aufl. 2011, Rn. 400; M. Bäcker, Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in: R. Uerpmann-Wittzack (Hrsg.), Das neue Computergrundrecht, Berlin Münster 2009, S. 1 (9); G. Britz, Grundsatzkritik (Fn. 1), S. 590.

23 Dabei liegt eine Herausforderung des neuen Grundrechtsaspekts allerdings darin, das persönliche Informationssystem angesichts der stetig steigenden Vernetzung auch persönlicher Datenspeicher im Einzelnen abzugrenzen.

24 M. Albers, Neukonzeption (Fn. 1), S. 121 ff.; dies.; Informationelle Selbstbestimmung (Fn. 1), S. 87 ff.; dies., Dimension (Fn. 1), S. 75; G. Britz, Grundsatzkritik (Fn. 1), S. 566 ff.

Auch der Schutz davor, dass Daten in einem Kontext zur Informationsgewinnung genutzt werden, ist als solches kein sinnvolles Schutzobjekt. Das Unfallopfer bedarf keines grundrechtlichen Schutzes davor, dass Daten über seinen aktuellen Puls und Blutdruck zur Gewinnung von Informationen für die anstehende Notoperation genutzt werden. So wie eine finanzielle staatliche Zuwendung keiner besonderen grundrechtlichen Rechtfertigung vor den Grundrechten des Empfängers bedarf, bedarf es ihr auch nicht bei der Datenerhebung zu seiner Rettung. Selbst die Gewinnung und Verwertung – besonders im europäischen Datenschutzkonzept – als besonders sensibel geltender Daten und Informationen über die Gesundheit muss nicht notwendig ein grundrechtliches Schutzbedürfnis auslösen. Das Abstellen auf die Informationsgewinnung allein kann bereits die allgemeine grundrechtliche Differenzierung zwischen rechtfertigungsbedürftigen grundrechtlichen Belastungen und grundrechtsfördernden Maßnahmen nicht leisten. Mit dem Hinweis auf den Verwendungskontext weist die Einbeziehung des Informationsgedankens aber in die Richtung, in der das Schutzgut der informationellen Selbstbestimmung zu suchen ist.

II. Das Recht auf informationelle Selbstbestimmung als reflexiver Grundrechtsschutz

Das Recht auf informationelle Selbstbestimmung will nicht vor Datenerhebungen, -speicherungen und darauf gestützter Informationsgewinnung als solcher schützen, sondern davor, dass durch sie Nachteile für die Grundrechtsentfaltung des Betroffenen entstehen.[26] Wenn der letztliche Zweck des Rechts auf informationelle Selbstbestimmung der Schutz vor Nachteilen ist, dann muss sich die Frage anschließen, auf welche Nachteile insoweit abgestellt werden soll. Hierzu zunächst drei Beobachtungen:

1. Kein „Doppelschutz“

Zunächst kann jedenfalls gesagt werden, welche Nachteile nicht gemeint sein können: nämlich die Nachteile, die sich mit der Anwendung von im Übrigen verfassungsmäßigen Eingriffsbefugnissen verbinden. Das Recht auf informationelle Selbstbestimmung soll nicht davor schützen, dass die zuständigen Behörden Informationen erhalten, die den Tatbestand von Rechtsnormen erfüllen und ihr Handeln in rechtmäßiger Weise programmieren. Der Schutz von Tagebüchern hat nicht den

25 Art. 8 Abs. 1 der sogenannten Datenschutz-Richtlinie 95/46/EG; s. aber auch § 3 IX BDSchG.

26 G. Britz, Grundsatzkritik (Fn. 1) S. 569 ff.; vgl. M. Eifert, Informationelle Selbstbestimmung im Internet, NVwZ 2008, S. 521 (523): Unterscheidung des Rechts auf informationelle Selbstbestimmung von den „letztlich geschützten Rechtsgütern“.

Zweck, Mörder vor der Überführung zu schützen sondern er muss in etwas anderem liegen. Es ist daher polemisch, wenn Bull gegen die Entscheidung des Bundesverfassungsgerichts zur videogestützten Geschwindigkeitskontrolle einwendet, dass die Kammer es als schutzwürdiges Interesse anzusehen scheint, „dass man nicht wegen seines Verhaltens im Straßenverkehr kontrolliert werden möchte."[27] Das Recht auf informationelle Selbstbestimmung will nicht davor schützen, dass Geschwindigkeitssünder die vom Gesetz vorgesehenen Bußen und Strafen erhalten. Gegen exzessive Geschwindigkeitsbegrenzungen schützen andere Grundrechte. Um einen Begriff von Marion Albers aufzugreifen: Das Recht auf informationelle Selbstbestimmung bietet keinen „Doppelschutz".[28]

2. Die Vielgestalt der Schutzziele

Mit dem Ausschluss des Doppelschutzes ist aber erst eine negative Annäherung gelungen. Die positive Antwort auf die Frage nach dem Schutzzweck des Rechts auf informationelle Selbstbestimmung fällt deshalb nicht einfach aus, weil das Recht auf informationelle Selbstbestimmung vor ganz unterschiedlichen Nachteilen schützt. In der US-amerikanischen Diskussion um den Datenschutz hat Daniel Solove eine Taxonomie der Gefahren entwickelt, die sich aus einem unzureichenden Datenschutz ergeben können, um dem Vorwurf entgegenzutreten, dass unklar sei, was das Recht auf Privatheit eigentlich schützen solle. Zu anämisch, zu abstrakt scheint seinen Kritikern ein allgemeines Datenschutzrecht. „Not enough dead bodies … lack of blood and death, or at least of broken bones and buckets of money."[29] lautet der Vorwurf.

Diesem Vorwurf will Solove mit seiner Taxonomie der Gefahren begegnen, die in fünf Kategorien fast zwei Dutzend Gefahren von irrtümlichen Beschuldigungen über soziale Exklusion und Vertrauensbruch bis zu Erpressung und Zudringlichkeit aufweist. Und er kann sogar auf vereinzelte tragische Fälle hinweisen, in denen ein unzureichender Datenschutz sehr wohl zu Toten geführt hat – wie etwa in dem Fall von Amy Lynn Boyer, deren Sozialversicherungsnummer und Arbeitsplatzadresse von einem Datenhändler an einen geistig verwirrten Verehrer verkauft wurde, der sie daraufhin an ihrem Arbeitsplatz aufsuchte und ermordete.[30]

---

27 H. P. Bull, Video-Verkehrskontrollen (Fn. 16), S. 3281.

28 M. Albers, Informationelle Selbstbestimmung (Fn. 1), S. 433: „Informations- und datenbezogene … Rechte … zielen … nicht auf eine Hinderung am Vollzug von Rechtsnormen und nicht auf einen ‚Doppel'-schutz. Hinter ihnen stehen vielmehr eigenständige Schutzziele."

29 A. Bartow, A Feeling of Uneasy about privacy law, University of Pennsylvania Law Review 155 (2006), PENNumbra, S. 52 (52, 62), http://www.pennumbra.com/responses/11-2006/Bartow.pdf (9.11.2006).

30 D. J. Solove, A Taxonomy of Privacy, University of Pennsylvania Law Review 154 (2006), S. 477 (530); ders., "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, San Diego Law Review 44 (2007), S. 745 (768).

Die Vielgestaltigkeit der Nachteile, welche die Taxonomie Soloves zusammenstellt, kann nicht wundern, wenn man den Hinweis auf den Verwendungskontext ernstnimmt. So unterschiedlich wie die Kontexte der Datennutzung sind auch die potenziellen Nachteile, vor denen das Recht auf informationelle Selbstbestimmung schützen soll. Je nach Art der Daten und je nach Verwendungskontext können sich aus der Verwendung von Daten ganz unterschiedliche Nachteile ergeben. Versucht man die Nachteile, um die es letztlich in den von Solove beschriebenen Szenarien geht, noch einmal zusammenzufassen, so geht es um drei Klassen von möglichen Schäden:

Erstens Opfer illegaler oder illegitimer Angriffe auf Rechtsgüter unterschiedlichster Art zu werden. Dies betrifft die Gefahr, Opfer eines Verbrechens zu werden, wenn etwa Bankdaten, Geheimnummern, aber auch nur Adressdaten – wie im Fall von Amy Lynn Boyer – in die Hände von Kriminellen, Konkurrenten oder Verwirrten fallen. Dies betrifft aber auch die Gefahr, Opfer von Diskriminierung[31] und sonstigen illegitimen Nachteilen zu werden, etwa im Kontakt mit Behörden, aufgrund von Informationen über politische Einstellungen,[32] sexuelle Orientierung etc.

Zweitens drohen negative Einwirkungen auf die Selbstdarstellung[33] – sowohl hinsichtlich des Fremd- als auch hinsichtlich des Selbstbildes –, die besonders durch das allgemeine Persönlichkeitsrecht als Teilrecht des Art. 2 Abs. 1 GG geschützt wird.[34] Dies betrifft die Gefahr der Beschädigung der Reputation, der Verzerrung oder auch nur Zementierung des Fremdbildes durch kompromittierende Informationen, die immer auch die Möglichkeit des Betroffenen einschränken, auf das Fremdbild Einfluss zu nehmen. Damit verwandt, aber doch davon verschieden, ist die Gefahr der Beschämung und Entwürdigung. Beides muss nicht notwendig reputationsschädigend sein, beides muss nicht notwendig das Fremdbild negativ beeinflussen, aber kann über – durch Scham erfahrbare – internalisierte Sozialnormen das

31 Diese erste Klasse von Nachteilen erfasst zunächst die ganz unmittelbaren Beeinträchtigungen durch Diskriminierungen – die Stelle, die jemand aufgrund von Informationen über seine sexuelle Orientierung, politische Haltung nicht bekommt etc. Zu den subtil über die Beschränkung von Horizonten der Selbstentwürfe wirkenden Beeinträchtigungen für die Selbstdarstellung durch Diskriminierungen G. Britz, Freie Entfaltung durch Selbstdarstellung. Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG, Tübingen 2007, S. 40 ff.

32 Vgl. BVerfGE 122, 342 (368 f.); zum erhöhten Risiko, Ermittlungsmaßnahmen aufgrund eines unberechtigten Verdachts ausgesetzt zu werden, BVerfGE 115, 320 (351); zur Gefährdung durch erhobene Daten ohne ausreichende Richtigkeitsgewähr BVerfGK 5, 32.

33 Dazu bereits N. Luhmann, Grundrechte als Institution, Berlin 1965, S. 53 ff.; G. Rüpke, Der verfassungsrechtliche Schutz der Privatheit, Baden-Baden 1976, S. 75 ff.; B. Schlink, Die Amtshilfe, Berlin 1982, S. 194 ff; ders., Das Recht auf informationelle Selbstbestimmung, Der Staat, 25 (1986), S. 233 ff.

34 Dieser Aspekt steht im Vordergrund der Rekonstruktion des Rechts auf informationelle Selbstbestimmung bei G. Britz, Selbstdarstellung (Fn. 31), S. 52 ff.; dies., Grundsatzkritik (Fn. 1).

35 D. J. Solove, Taxonomy (Fn. 30), S. 486 f.

Selbstbild beeinträchtigen. Die Veröffentlichung eines Nacktfotos muss nicht reputationsschädigend sein, kann aber trotzdem beschämen.

Drittens sind es informatorische Machtasymmetrien, die bereits als solche die Handlungsoptionen des Betroffenen einschränken oder ihn sogar ohnmächtig und damit einer fremden Macht gefügigmachen können und wie die illegalen Übergriffe eine Vielzahl von Rechten und Rechtsgütern betreffen können: die Verhandlungsstrategie in den Händen des Verhandlungsgegners,[36] das Gefühl der Ohnmacht gegenüber der Behörde, die über ausgedehnte Persönlichkeitsprofile verfügt,[37] das Ausgeliefertsein gegenüber einer umfassenden Überwachung.[38]

Die Furcht vor den drei Nachteilstypen, in ihren vielfältigen Ausprägungen, Überschneidungen und Kombinationen bringt noch einen vierten Nachteil hervor: die Selbstbeschränkung, die Inhibition, die die Entfaltungsmöglichkeiten des Grundrechtsträgers noch zusätzlich beeinträchtigt, indem sie bereits Handlungsimpulse erstickt.[39] Wer weiß, dass seine Versammlungsteilnahme staatlich registriert wird, muss fürchten, Opfer von Diskriminierung zu werden und verzichtet deshalb bereits auf die Teilnahme. Wer weiß, dass exaltiertes Benehmen im öffentlichen Raum videographiert wird, muss um seine Reputation fürchten, wenn die Daten dem Dienstvorgesetzten oder Arbeitgeber in die Hände fallen können, und schränkt die Entfaltung seiner Persönlichkeit an entsprechenden Orten ein.

Neben dieser „äußeren" Seite kann die Inhibition aber auch eine „innere" aufweisen.[40] Beeinträchtigungen der Handlungsfreiheiten, der Selbstdarstellung und der Selbstentwürfe sind auch deshalb grundrechtlich relevant, weil sie in direkter Beziehung zur individuellen[41] Autonomie stehen. Die Freiheit, die das Grundgesetz

36 Vgl. BVerfGK 9, 353, zur Verletzung des Rechts auf informationelle Selbstbestimmung durch eine in Versicherungsverträgen enthaltene generelle Verpflichtung, zur Feststellung des Versicherungsfalls eine Schweigepflichtentbindung zu erteilen.

37 Zur Gefährdung durch die Verknüpfung von Datenbeständen BVerfGE 65, 1 (42); 115, 320 (342); 118, 168 (184 f.); 120, 274 (311 f.); 120, 378 (397 f.); dazu G. Britz, Grundsatzkritik (Fn. 1), S. 576; M. Albers, Umgang (Fn. 1), Rn 76; krit. gegenüber der Gefahr durch so genannte Persönlichkeitsprofile H.-H. Trute, Grundlagen (Fn. 1), Rn. 26; K. H. Ladeur, Fehlkonstruktion (Fn. 1), S. 52.

38 BVerfGE 125, 260 (333 f.).

39 Zu derartigen Einschüchterungseffekten bereits BVerfGE 65, 1 (42 f.); ferner BVerfGE 34, 238 (246 f.); 93, 181 (188); 100, 313 (381); 107, 299 (328); 109, 279 (354); 113, 29 (46); 115, 166 (188); 115, 320 (354 f.); 118, 168 (203 f.); 120, 378 (402); 125, 260 (332); G. Britz, Grundsatzkritik (Fn. 1), S. 569 ff.; J. H. Klement, Die Kumulation von Grundrechtseingriffen im Umweltrecht, AöR 134 (2009), S. 35 (46 ff.); C. Rath, Karlsruhe und der Einschüchterungseffekt – Praxis und Nutzen einer Argumentationsfigur des Bundesverfassungsgerichts, in: Kritische Justiz (Hrsg.), Verfassungsrecht und gesellschaftliche Realität, Baden-Baden 2009, S. 65.

40 Zu der äußeren und inneren Seite des Grundrechts aus Art. 2 Abs. 1 GG, G. Britz, Selbstdarstellung (Fn. 31), S. 16 ff., 23 ff.

41 Zum Verhältnis von individueller personaler und kollektiver demokratischer Autonomie B. Rössler, Der Wert des Privaten, Frankfurt a. M. 2001, S. 234.

schützt, ist nicht die bloße Auswahlfreiheit des „choosers“[42], sondern die Autonomie der Grundrechtsträger als Personen, die ihre Entscheidungen im Lichte der eigenen Geschichte und vor dem Hintergrund von Selbstentwürfen für sich begründen.[43] Beschränkungen der Handlungsfreiheit und manipulierte, verzerrte, für den Betroffenen intransparente oder zementierte Fremdbilder, wie sie durch den unkontrollierten Zugang zu personenbezogenen Daten begünstigt werden, beeinträchtigen jedoch die Bedingungen für eine als personale[44] Autonomie verstandene Freiheit. Indem sie die erfolgreiche Selbstdarstellung erschweren oder sogar unmöglich machen, beschränken sie bereits den Möglichkeitsraum der Selbstentwürfe. Jemand der aufgrund eines über ihn kursierenden Persönlichkeitsprofils in einem bestimmten Berufsfeld keine Chancen mehr hat, wird u. U. auch seinen Selbstentwurf entsprechend anpassen. Er wird seine Handlungsoptionen schon nicht mehr vor dem Hintergrund eines ihm sonst möglichen Selbstentwurfs bewerten und damit ein Stück seiner personalen Autonomie einbüßen.

Die Selbstzensur ist auch der Grund dafür, warum eine exzessive Überwachung, die lediglich der als solche legitimen Ahndung von Rechtsverstößen dient, mit Nachteilen verbunden ist, vor denen das Recht auf informationelle Selbstbestimmung schützen will. Das Recht auf informationelle Selbstbestimmung schützt nicht vor der Ahndung von Rechtsverstößen. Aber eine exzessive Überwachung führt zu Formen der Selbstbeschränkung, die dann auch rechtmäßiges Verhalten betreffen, das jedenfalls durch die allgemeine Handlungsfreiheit und das allgemeine Persönlichkeitsrecht geschützt ist. Wer fürchten muss, dass jede kleinste Normübertretung registriert und geahndet wird, wird in sein Verhalten einen Sicherheitsabstand zu dem noch Erlaubten einbauen. Wären alle Kraftfahrzeuge mit einem GPS-gestützten Geschwindigkeitssensor ausgerüstet, der in der geschlossenen Ortschaft bei Tempo 51 km/h die Fahrzeugdaten an das Ordnungsamt und nach Flensburg meldete, führen die meisten allenfalls noch 45 km/h. Eine exzessive Überwachung führt zu einem vorauseilenden Verzicht auf die Ausübung grundrechtlicher Freiheit und Autonomie und damit besonders auch zu einer Verflachung der in Art. 2 Abs. 1 GG allgemein geschützten Persönlichkeitsentfaltung.

Darin liegt auch eine der besonderen Gefahren der Vorratsdatenspeicherung. Durch die Vorratsdatenspeicherung der IP-Adressen kann rekonstruiert werden, wer eine Internetseite wann, für welche Dauer und in welcher Intensität genutzt hat. In der realen Welt entspräche dem, dass sich jeder Blick in ein Schaufenster und jede

42 B. Rössler, ebd., S. 95.

43 B. Rössler, ebd., S. 83 ff., 124, auch eingehend zum Zusammenhang von Privatheit, Selbstdarstellung und Autonomie; daran anknüpfend für eine Konzeption des allgemeinen Persönlichkeitsrechts als Recht auf Selbstdarstellung G. Britz, Selbstdarstellung (Fn. 31), S. 9 ff.

44 Personale Autonomie ist von moralischer zu unterscheiden, s. dazu B. Rössler, Wert (Fn. 41), S. 99: Personale Autonomie muss nicht in moralischer aufgehen. Man kann sich auch gegen moralische Standards entscheiden. Doch die moralischen Gründe gehen immer schon in die personal autonome Entscheidung ein.

Berührung eines Gegenstands in einem Warenhaus oder einer Bibliothek anhand einer zentralen Iris- und Fingerabdruckdatei rekonstruieren ließe. Dass diese Art der Totalüberwachung der virtuellen Welt nicht unproblematisch ist, wenn sie wegen jeglicher Normüberschreitung aktualisiert werden kann, hat auch das Bundesverfassungsgericht gesehen. Es hat daher die Zulässigkeit entsprechender Rekonstruktionen mittels der Vorratsdatenspeicherung beschränkt. Wenn nicht wegen jedem Normverstoß, sondern nur wegen besonders gravierender mit einer Rekonstruktion der Seitenaufrufe gerechnet werden muss, ließen sich die Inhibitionseffekte, die von der Vorratsdatenspeicherung ausgehen, begrenzen. Ob allerdings die Beschränkung auf „Ordnungswidrigkeiten von besonderem Gewicht“[45] hierfür ausreicht, scheint mehr als fraglich.

Das Recht auf informationelle Selbstbestimmung hat instrumentellen Charakter.[46] Es dient nicht dem Schutz eines eigentumsähnlich verstandenen Rechts an Daten oder grundsätzlich der Verhinderung personenbezogener Informationen, sondern es gilt der Verhinderung von Nachteilen für die Entfaltung grundrechtlicher Freiheit und Autonomie, die sich aus der Verwendung von Daten ergeben können. Das Recht auf informationelle Selbstbestimmung ist auf den Schutz anderer – von ihm selbst verschiedener – Grundrechtspositionen gerichtet. Es ist – anders als die meisten anderen Grundrechte –[47] nicht Selbstzweck, sondern ein reflexives – aber nicht selbstreflexives – Grundrecht zum Schutz anderer Grundrechtspositionen.

III. Informationelle Selbstbestimmung als Schutz vor Grundrechtsgefährdungen

Diese anderen Grundrechtspositionen werden durch Datenerhebungen und -speicherungen zur Informationsgewinnung aber regelmäßig nicht unmittelbar beeinträchtigt. Weder die Datenerhebung noch ihre Interpretation als solche führt bereits zu den beschriebenen Nachteilen, regelmäßig ergeben sie sich erst durch weitere Interaktionen. Dies weist auf eine zweite Besonderheit des Rechts auf informationelle Selbstbestimmung hin. Indem es bei der Datenerhebung, -speicherung und -verarbeitung ansetzt, erfasst es bereits die Gefährdung der Grundrechtspositionen, denen Nachteile drohen. Griffe das Recht auf informationelle Selbstbestimmung erst bei der Beeinträchtigung dieser anderen Positionen, wäre es redundant, da die durch die Nachteile betroffenen Grundrechte dann selbst Schutz böten. Das Recht auf informationelle Selbstbestimmung schützt demgegenüber bereits vor den spezifischen Gefährdungen grundrechtlicher Freiheit, Autonomie und Gleichheit durch aus Daten abgeleitete Informationen.

45 BVerfGE 125, 260 (344), Ls. 6.

46 G. Britz, Grundsatzkritik (Fn. 1), S. 571: „akzessorisches Recht“.

47 Eine ähnliche Struktur weisen noch die ebenfalls an dem Schutz der Privatsphäre orientierten Grundrechte aus Art. 10 u. 13 GG sowie das neu geschaffene „Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme“ auf, vgl. dazu oben Fn. 22.

Dass das Recht auf informationelle Selbstbestimmung bereits bei der Gefährdung, also im Vorfeld der Informationsgewinnung ansetzen muss, folgt nicht zuletzt aus der eigenartigen Struktur des Gutes „Information", die auch die Informationsökonomie beschäftigt. Den Wert von Informationen kann erst bemessen, wer sie kennt. Kennt man sie, entfällt aber der Anreiz zu ihrem Erwerb. Die Kehrseite dieser informationsökonomischen Einsicht liegt darin, dass der Schutz vor dem Erwerb von Informationen zu spät kommt, wenn die Information erst einmal erfolgt ist.[48] Der Schutz vor der Information muss daher bereits bei dem Schutz der Daten ansetzen. Das Recht auf informationelle Selbstbestimmung ist daher zutreffend als ein Recht beschrieben worden, das vor Grundrechtsgefährdungen durch die Verwendung von Daten schützen soll. Es schützt andere Grundrechtspositionen vor Gefährdungen. Insoweit ist es ganz zutreffend, wenn Ladeur die Nähe des Rechts auf informationelle Selbstbestimmung zum Risiko- und Vorsorgerecht betont,[50] zumal es in der Regel auch nicht der Abwehr konkreter, sondern abstrakter Gefahren[51] gilt.

48 M. Eifert, Internet (Fn. 26), S. 523; zur Informationsökonomie M. Hutter, Ökonomische Eigenheiten des e-Commerce, AfP 31 (2000), S. 30.

49 Vgl. entsprechende Ansätze bereits bei H.-U. Gallwas, Verfassungsrechtliche Grundlagen des Datenschutzes, Der Staat 18 (1979), S. 507 (514); im Anschluss an das Volkszählungsurteil R. Scholz/R. Pitschas, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin 1984, S. 83 f.; C. Karaus, Der grundrechtliche Schutz der Privatsphäre bei der Erhebung, Verarbeitung und Weitergabe von statistischen Daten, Berlin 1985, S. 64; aus der neueren Literatur in sozialphilosophischer Perspektive B. Rössler, Wert (Fn. 41), S. 230, die entscheidend darauf abstellt „wie wahrscheinlich tatsächlich folgende Freiheitsbeschränkungen wären; wie sehr der individuelle Alltag im Sinne alltäglicher sozialer Praktiken (im Gegensatz zu Ausnahmesituationen) betroffen wäre."; aus dogmatischer Sicht eingehend G. Britz, Grundsatzkritik (Fn. 1), S. 582. Kritisch auch zu weiteren Ansätzen, die die informationelle Selbstbestimmung in Richtung eines Grundrechtsvoraussetzungsschutzes deuten, M. Albers, Informationelle Selbstbestimmung (Fn.1), S. 156 f., 602. Albers liegt daran, den Selbstand des Rechts auf informationelle Selbstbestimmung zu betonen, der aber entgegen ihren Bedenken auch in dem spezifischen Gefährdungsschutz gesehen werden kann.

50 K. H. Ladeur, Fehlkonstruktion (Fn. 1), S. 53 f.

51 Zu einzelnen Konstellationen des Vorfeldschutzes G. Britz, Grundsatzkritik (Fn. 1), S. 578 ff.

C. Dogmatische Konsequenzen

Welche dogmatischen Konsequenzen lassen sich aus der Rekonstruktion des Rechts auf informationelle Selbstbestimmung als ein reflexives Grundrecht auf Abwehr von Grundrechtsgefährdungen durch den Umgang mit Daten ziehen?

I. Der Schutzbereich des Rechts auf informationelle Selbstbestimmung

1. Breite grundrechtliche Aufmerksamkeit

Es spricht wegen der Abhängigkeit der Gefährdung vom Verwendungskontext zunächst nichts dagegen, den Schutzbereich des Rechts auf informationelle Selbstbestimmung auch weiterhin bei der Erhebung, Speicherung und Verwertung von personenbezogenen Daten für einschlägig zu erachten.[52] Die weite Anlage des Schutzbereichs, der nur durch das Merkmal der Personenbezogenheit der Daten beschränkt ist, kann auch bei einem Verständnis des Rechts auf informationelle Selbstbestimmung als eines Gefährdungsabwehrrechts dafür sorgen, dass zunächst allen potenziell in Betracht kommenden Gefährdungen grundrechtliche Aufmerksamkeit zuteilwird. Die Weite seines Schutzbereichs entspricht der grundsätzlichen Zuordnung des Rechts auf informationelle Selbstbestimmung zu Art. 2 Abs. 1 GG. Dabei kann sich der Gefährdungsschutz sowohl auf die allgemeine äußere Handlungsfreiheit als auch auf das allgemeine Persönlichkeitsrecht in Gestalt personaler Autonomie und Selbstdarstellung beziehen. Die Besonderheit des Schutzbereichs der informationellen gegenüber den allgemeinen Aspekten von Art. 2 Abs. 1 GG liegt eben darin, dass personenbezogene Daten bereits aufgrund ihres Gefährdungspotenzials zu einem selbständigen Schutzaspekt ausgestaltet werden.

2. Zuordnung von Gefährdungen zu speziellen Schutzbereichen

Das Abstellen auf die Gefährdung bietet auch die Möglichkeit, eine Datenerhebung oder Speicherung dem Schutzbereich eines speziellen Grundrechts zuzuordnen. Soweit sich weder aus den Daten noch aus den im Raum stehenden Gefährdungen ein besonderer Bezug zu einem spezifischen Grundrecht ergibt, bliebe der Schutzbereich des allgemeinen Rechts auf informationelle Selbstbestimmung einschlägig. Ergibt sich aber eine Gefährdung, die einen besonderen Bezug zu einem spezielleren Grundrecht aufweist, so ist der Schutzbereich des jeweils spezielleren Eingriffs ein-

52 So auch G. Britz, Grundsatzkritik (Fn. 1), S. 582.

schlägig.[53] Bild- und Tonaufnahmen bei Versammlungen, die sich negativ auf die „innere Versammlungsfreiheit" potenzieller Versammlungsteilnehmer auswirken, sind danach an Art. 8 GG zu messen. So hat das Bundesverfassungsgericht seine einstweilige Anordnung zu den Regelungen der Videoüberwachung des bayerischen Versammlungsgesetzes auf deren negative Folgen für die Versammlungsfreiheit gestützt.[54]

Über die Zuordnung zu speziellen Schutzbereichen werden auch deren besondere Rechtfertigungsanforderungen aktiviert. Für die Versammlungsfreiheit etwa die besonderen Eingriffsschwellen für Versammlungen unter freiem Himmel auf der einen und für solche in geschlossenen Räumen auf der anderen Seite.[55] Werden Daten zur politischen Betätigung von Personen gesammelt, um sie auf ihre Staatsfeindlichkeit einzuschätzen, ist die Meinungsfreiheit und damit auch das Verbot sonderrechtlicher Maßnahmen einschlägig.[56] Über das Abstellen auf die Spezifik von Gefährdungen, die sich aus der Erhebung, Speicherung und Verwendung von Daten ergeben, lässt sich das Recht auf informationelle Selbstbestimmung auch spezialgrundrechtlich verorten.

II. Grundrechtsgefährdungen als Grundrechtseingriff

Ein Verständnis, das jede Erhebung, Speicherung und Verwendung von Daten als Grundrechtseingriff versteht, das den Grundrechtseingriff von den Gefährdungen abkoppelt und jeden Umgang mit Daten den grundrechtlichen Rechtfertigungsanforderungen unterwirft, läuft Gefahr, zu eben jenen Verselbständigungen zu führen, die die Kritiker des Rechts auf informationelle Selbstbestimmung ihm gegenüber in Stellung bringen. Zudem werden Differenzierungen verspielt, die in der allgemeinen Grundrechtsdogmatik angelegt sind.

1. Nachteilige und vorteilhafte Einwirkungen

Eine erste Differenzierung wurde bereits angesprochen. Wenn für den Eingriff in das Recht auf informationelle Selbstbestimmung lediglich auf die Erhebung, Speicherung und Verwertung von Daten abgestellt wird, kann die sonst für den Ein-

53 J. Masing, Gesetz und Gesetzesvorbehalt – zur Spannung von Theorie und Dogmatik am Beispiel des Datenschutzrechts, in: W. Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, Tübingen 2010, S. 467 (482).

54 BVerfGE 122, 342 (368 f.).

55 Für ein entsprechend differenzierendes Regelungsmodell s. etwa C. Enders/W. Hoffmann-Riem/M. Kniesel/R. Poscher/H. Schulze-Fielitz, Musterentwurf eines Versammlungsgesetzes, München 2011, S. 46 ff.; S. 72 ff.

56 Zu dem entsprechenden Beispiel M. Albers, Informationelle Selbstbestimmung (Fn. 1), S. 423.

griffsbegriff konstitutive Unterscheidung zwischen für den Grundrechtsträger vorteilhaften und nachteiligen Einwirkungen auf den Schutzbereich nicht abgebildet werden. Eine Datenerhebung träfe auch dann die grundrechtliche Rechtfertigungslast, wenn sie lediglich zum Vorteil des Betroffenen – etwa zur Rettung aus einer Not – diente und sich auch sonst keine Gefahren aus ihr ergäben. Zunächst müsste für einen Eingriff in das Recht auf informationelle Selbstbestimmung also dargetan werden, dass es durch die Erhebung, Speicherung und Verwendung eines Datums überhaupt zu einer Gefährdung grundrechtlicher Freiheitsentfaltung kommt, die nicht allein in der Anordnung einer rechtlich vorgesehenen Rechtsfolge liegt.

2. Gefährdungsintensität als Eingriffskriterium

In der allgemeinen Eingriffsdogmatik wird bei faktischen Grundrechtseingriffen weiterhin zwischen Eingriffen und Beeinträchtigungen des Schutzbereichs unterschieden, die nicht die Intensität eines Eingriffs erreichen. Durch die Erweiterung des klassischen Eingriffsbegriffs und die Aufgabe der Kriterien „final" und „imperativ" geraten alle Folgewirkungen staatlicher Maßnahmen, die sich nachteilig auf einen grundrechtlichen Schutzbereich auswirken, in den Blick der Eingriffsdogmatik und wären den entsprechenden Rechtfertigungsanforderungen ausgesetzt. Um sowohl den Gesetzgeber mit der Schaffung entsprechender Ermächtigungsgrundlagen und die Gerichte mit entsprechenden Verfahren nicht zu überfordern, wird kompensatorisch eine gewisse Intensität der faktischen grundrechtlichen Beeinträchtigung für die Annahme eines Grundrechtseingriffs verlangt.[57] Bestimmte nachteilige Folgewirkungen staatlicher Maßnahmen auf den Schutzbereich eines Grundrechts sind so alltäglich und so geringfügig, dass sie die Schwelle eines Grundrechtseingriffs nicht überschreiten. Bestimmte Geräuschimmissionen oder Geruchsimmissionen können zwar schon das Wohlbefinden beeinträchtigen, erreichen aber noch nicht die Schwelle des Grundrechtseingriffs. Wenn die Polizei eine Kontrollstelle einrichtet und sich dadurch der Verkehr so staut, dass wir in unserer Bewegungsfreiheit beschränkt werden, liegt darin noch kein Grundrechtseingriff.

Bei den Nachteilen, vor denen das Recht auf informationelle Selbstbestimmung schützen will, handelt es sich regelmäßig weder um final angestrebte noch um imperativ angeordnete Nachteile, sondern um faktische Folgewirkungen von Datenerhebungen und -speicherungen, bei denen bereits die allgemeine Grundrechtsdogmatik

57 A. Scherzberg, Grundrechtsschutz und „Eingriffsintensität", Berlin 1989, S. 206 f.; R. Eckhoff, Der Grundrechtseingriff, Köln u. a. 1992, S. 255 ff.; B. Pieroth/B. Schlink, Grundrechte (Fn. 22), Rn. 260; a. A. K. Stern, Das Staatsrecht der Bundesrepublik Deutschland, Bd. III/2, München 1994, S. 205 ff. m. w. N.

für die Annahme eines Eingriffs eine gewisse Intensität der Beeinträchtigung verlangt.[58]

Hinzu kommt, dass der Schutz des Rechts auf informationelle Selbstbestimmung bereits bei Gefährdungen einsetzt. Gefährdungen beruhen auf graduell skalierten Wahrscheinlichkeiten eines Schadenseintritts. Dabei kann eine relevante Gefährdung nur angenommen werden, wenn sie das allgemeine Lebensrisiko überschreitet. Für das Maß der erforderlichen Überschreitung des allgemeinen Lebensrisikos muss die Wahrscheinlichkeit zudem in ein Verhältnis zu der Bedeutung des drohenden Nachteils gesetzt werden. Bereits aus diesem Grund kann nicht in jeder Nachteilswahrscheinlichkeit ein Grundrechtseingriff liegen. Dies gilt für die informationelle Selbstbestimmung wie für andere Grundrechtspositionen. Wenn Polizei oder Feuerwehren mit Sonderrechten fahren, besteht eine höhere Unfallgefahr auch für die übrigen Verkehrsteilnehmer. Trotzdem liegt in dieser Gefährdung noch kein Eingriff in deren körperliche Unversehrtheit.

Daher können Gefährdungen, die mit Datenerhebungen oder -speicherungen verbunden sind, auch dort, wo es sie gibt, aus zwei Gründen unterhalb der Eingriffsschwelle liegen: Zum einen dann, wenn die Wahrscheinlichkeit des Schadenseintritts niedrig und dem allgemeinen Lebensrisiko angenähert ist; zum anderen, wenn selbst bei Eintritt der befürchteten Nachteile der Schaden so gering wäre, dass er unter der Erheblichkeitsschwelle bleibt. Deshalb verbinden sich etwa mit den traditionellen Streifengängen von Polizisten, bei denen jede Menge Daten erhoben werden, keine Eingriffe in das Recht auf informationelle Selbstbestimmung – auch dann nicht, wenn die Streifengänge regelmäßig erfolgen und den Beamten Einblicke in die Lebensgewohnheiten der Betroffenen geben[60]. Die mit den gelegentlichen Datenerhebungen verbundenen Gefährdungen sind zu gering, die Gefahren zu alltäglich und sie unterscheiden sich strukturell zu wenig von denen, denen wir durch Nachbarn, Anwohner und Postboten ausgesetzt sind.

Nichts anderes dürfte für die bislang üblichen punktuellen Radarfallen gelten, die lediglich die Geschwindigkeitssünder erfassen und – anders als neuere Verfahren der Streckenüberwachung –[61] nicht den gesamten Verkehr registrieren. Der Nachteil, dem das Recht auf informationelle Selbstbestimmung gilt, ist insoweit nicht die Sanktion für die Geschwindigkeitsüberschreitung. Andere – jedenfalls signifikante –

58 Zur fehlenden Eingriffsqualität bloßer informatorischer Belästigungen auch F. Schoch, Das Recht auf informationelle Selbstbestimmung, Jura 2008, S. 352 (357); vgl. auch W. Hoffmann-Riem, Informationsgesellschaft (Fn. 1), S. 529 ff., der sich zu Recht gegen einen pauschalen Bagatellvorbehalt für bestimmte Daten ausspricht und darauf verweist, dass sich auch die Eingriffsintensität in erster Linie nach den Verwendungskontexten richtet.

59 Eine Typologie eingriffsrelevanter Gefährdungen bei G. Britz, Grundsatzkritik (Fn. 1), S. 579 ff.

60 H. P. Bull, Video-Verkehrskontrollen (Fn. 16), S. 3282.

61 Dazu C. Arzt/J. Eier, Section Control und allgemeine Videoüberwachung im Straßenverkehr – Neue und alte Maßnahmen ohne Rechtsgrundlage, NZV 2010, S. 113.

Gefährdungen, die von den punktuellen personenbezogenen Geschwindigkeitsdaten ausgehen, sind jedoch nicht ersichtlich. Auch empirisch sind trotz ihres jahrzehntelangen Einsatzes weder Missbrauchsfälle noch Selbstdarstellungsnachteile noch Machtasymmetrien bekannt geworden, die zur Inhibition grundrechtlich geschützter Persönlichkeitsentfaltung führen. Das allgemeine Geschwindigkeitsniveau bewegt sich vielmehr immer noch eher etwas über als unter dem nach der StVO jeweils zulässigen Maß.

a) Technologische Entwicklungen

Die Differenzierung zwischen Eingriff und bloßer Beeinträchtigung bietet auch eine Möglichkeit, das Recht auf informationelle Selbstbestimmung den sich wandelnden sozialen und technischen Bedingungen anzupassen. Dabei kann die Anpassung in beide Richtungen erforderlich sein:

Zum einen kann sich besonders die technische Entwicklung so auswirken, dass sie Gefährdungen verstärkt. So wurde das Recht auf informationelle Selbstbestimmung gerade angesichts der neuen Gefahren, die von der elektronischen Datenverarbeitung ausgehen, überhaupt erst entwickelt. Heute können etwa die zunehmenden inferenziellen Möglichkeiten, die sich durch erhobene und öffentlich zugängliche Daten bieten, zu einer Steigerung der Gefährdung führen, wenn ihnen nicht durch entsprechende Regulierungen begegnet wird. Ein weiteres Beispiel aus der Rechtsprechung bieten Übersichtsaufnahmen bei Versammlungen: „Dabei ist die Anfertigung solcher Übersichtsaufzeichnungen nach dem heutigen Stand der Technik für die Aufgezeichneten immer ein Grundrechtseingriff, da auch in Übersichtsaufzeichnungen die Einzelpersonen in der Regel individualisierbar mit erfasst sind.“[62] Mit einer Steigerung der technischen Möglichkeiten zur automatisierten Gesichtserkennung wird sich dieser Befund noch verstärken.

Zum anderen können aber auch Gegentechnologien entwickelt werden, die sich mindernd auf die Eingriffsintensität oder sogar auch -relevanz von Datenerhebungen auswirken. So werden etwa Varianten der anonymisierten Videoüberwachung entwickelt, die die Möglichkeit eröffnen, Kriterien für die Reanonymisierung zu bestimmen. Zusammen mit einem rechtlichen und technologischen Regime, das ausreichend enge Zweckbegrenzungen – etwa auf die Verhütung und Verfolgung schwerster Straftaten –[63] effektiv absichert und überwacht, ergäbe sich eine ganz andere Beurteilung der Eingriffsintensität als bei heutigen Überwachungen.

62 BVerfGE 122, 342 (368 f.).

63 Vgl. demgegenüber die ausufernden Kataloge etwa in § 100a Abs. 2 StPO oder den Landespolizeigesetzen, s. etwa § 22 Abs. 5 PolG BW, § 8 Abs. 3 PolG NRW.

b) Gesellschaftliche Veränderungen

Als Gefährdungsabwehrrecht kann das Recht auf informationelle Selbstbestimmung auch gesellschaftlichen Veränderungen im Umgang mit persönlichen Daten Rechnung tragen. Gesellschaftliche Veränderungen können die erheblichen Gefährdungen, mit denen Datenerhebungen und -speicherungen bislang verbunden sind, entfallen lassen, unter die Erheblichkeitsschwelle drücken oder jedenfalls deren Intensität deutlich absenken. Insoweit könnten etwa die eingangs genannten Verschiebungen im Verhältnis von Privatheit und Öffentlichkeit von Belang sein.

Wenn Norbert Elias auch nur im Ansatz Recht mit seiner These hat, dass unsere heutigen Vorstellungen von Privatheit historisch der zunehmenden sozialen Verflechtung geschuldet sind, die mit einer gewissen funktionalen Notwendigkeit starke Affekte, Emotionen und tierische Aspekte der Körperlichkeit aus der Öffentlichkeit ausschließt,[64] ist allerdings nicht davon auszugehen, dass in unseren hochgradig interdependenten Gesellschaften ein Ende der Privatheit droht. Was jedoch auch Elias für möglich erachtete, sind Schwankungen und Verschiebungen dessen, was aus der Öffentlichkeit ausgeschlossen und – etwa über als Scham internalisierte Sozialnormen – in den Bereich des Privaten abgedrängt wird.[65]

Ähnliches gilt auch für den Zusammenhang von Autonomie und Privatheit. Wenn sich der Zusammenhang auch nur im Ansatz als notwendig erweist, wird mit dem Bedürfnis nach Autonomie auch das Bedürfnis nach Privatheit lebendig bleiben. Doch zum einen sind die konkreten Bedingungen der Privatheit in hohem Maße konventionell.[66] Autonomie ist auf Formen der informationellen Privatheit angewiesen, auf die die Selbstdarstellung sich einstellen kann und die ihr noch Wirkungschancen belassen. Doch gerade unter Bedingungen von Transparenz sind die Formen der Privatheit variabel. Zum anderen sind sowohl Privatheit als auch Autonomie graduelle Phänomene, für die u. U. auch die Nachfrage schwanken kann. Auch im Blick auf die personale Autonomie kann es daher zu Verschiebungen der Privatheit kommen.

Solche Verschiebungen, wie wir sie zurzeit jedenfalls in Ansätzen beobachten, verschieben auch die Gefährdungen, die von Datenerhebungen und -speicherungen ausgehen – besonders soweit sie Gefahren für die Selbstdarstellung betreffen. Wenn Daten, die heute noch zu einer Bloßstellung taugen, künftig so öffentlich behandelt werden, dass auch ihre staatliche Kenntnisnahme und Speicherung keine über das informationelle Alltagsrisiko hinausgehende Gefahren für die Autonomie und Selbstdarstellung mehr birgt, könnte ein Eingriffsverständnis, das auf die Grundrechtsgefährdung abstellt, dieser Entwicklung Rechnung tragen. Ohne seine Struktur

64 N. Elias, Über den Prozess der Zivilisation, Bd. 2, Frankfurt u. a. 1991, S. 312 ff., 397 ff.

65 Vgl. zu diesem Vorgang allgemein N. Elias, ebd., S. 397 ff.; exemplarisch zur Intimisierung des Schlafens und zum Verhältnis der Geschlechter ders., Über den Prozess der Zivilisation, Bd. 1, Frankfurt u. a. 1991, S. 227 ff., 230 ff.

66 B. Rössler, Wert (Fn. 41), S. 212 f.

zu verändern, kann sich ein als reflexives Grundrecht zur Abwehr von Freiheitsgefährdungen verstandenes Recht auf informationelle Selbstbestimmung an die gesellschaftlichen Veränderungen anpassen.

Dabei wird man jedoch vorsichtig sein müssen, eine entsprechende Verschiebung anzunehmen. Zum einen kann für die Annahme einer entsprechenden Verschiebung nicht allein das Empfinden einer bestimmten Jugendkultur maßgeblich sein. Zum anderen liegen noch zu wenige Erfahrungen über die langfristigen Folgen der Datenfreizügigkeit vor, die von den Propheten des Endes der Privatheit gefeiert wird. Aber selbst wenn Norbert Elias falsch liegen sollte und wir den Prozess der Zivilisation doch umkehren könnten, hätte das Recht auf informationelle Selbstbestimmung bis zu dem prophezeiten Ende der Privatheit noch eine wichtige katechontische Funktion.[67]

c) Veränderungen des Wissens

Offen ist das Recht auf informationelle Selbstbestimmung auch für epistemische Veränderungen. Die Gefährdungen, auf die dieses Verständnis abstellt, beruhen letztlich auf empirischen Prognosen und lassen sich damit jedenfalls grundsätzlich empirisch überprüfen. So wird etwa der Einschüchterungseffekt von Rasterfahndungen und Videoüberwachungen in Frage gestellt.[68] Zuzugeben ist dieser Kritik, dass viele der Gefahren, die mit staatlichen Datenerhebungen und -speicherungen verbunden werden, auf Alltagstheorien beruhen, die zwar eine gewisse lebensweltliche Plausibilität haben, aber selten auf empirisch validen Daten beruhen. Auch wenn es eine kaum zu unterschätzende Herausforderung für die empirische Sozialforschung ist, so komplexe und volatile soziale Mechanismen wie Einschüchterungseffekte zu untersuchen, ist es doch nicht ausgeschlossen, dass wir entweder lernen, dass es reale Gefahren dort gibt, wo wir sie nicht vermutet haben, oder dass Gefahren, von denen wir immer ausgegangen sind, weniger dramatisch ausfallen. Das vorgeschlagene Eingriffskonzept ist also nicht nur offen für einen Wandel der Gesellschaft, sondern auch für einen Fortschritt unserer Erkenntnisse über dieselbe.

67 Zur katechontischen Funktion des Technikrechts B. Schlink, Die Bewältigung der wissenschaftlichen und technischen Entwicklung durch das Verwaltungsrecht, VVDStRL 48 (1990), S. 235 (259 ff.).

68 H. P. Bull, Informationskultur (Fn. 1), S. 54; ders., Vision oder Illusion (Fn. 1), S. 61 ff.; vgl. auch die Kritik der beiden abweichenden Meinungen in der Entscheidung zur Vorratsdatenspeicherung bzgl. behaupteter Einschüchterungseffekte, BVerfGE 125, 260 (364 ff. u. 380 ff.).

d) Zweckbegrenzung

Bereits auf der Ebene des Eingriffs muss auch die Zweckbegrenzung mit ins Auge gefasst werden. Nur über die Begrenzung der Verwendungszwecke lassen sich die Gefahren absehen, die von einer Datenerhebung und -speicherung ausgehen können. Nur wenn die Verwendungskontexte bestimmt sind, lassen sich Missbrauchsgefahren abschätzen. Auch soweit legitime Verwendungen im Raum stehen, aber nicht transparent sind, können intransparente Verwendungsmöglichkeiten diffuse Überwachungsgefühle auslösen, die wiederum zu einer Selbstbeschränkung der freien Entfaltung der Persönlichkeit führen können. Das Recht auf informationelle Selbstbestimmung schützt zwar nicht davor, dass der Staat Informationen erlangt, die nach den rechtlichen Handlungsprogrammen der Behörden nachteilige Rechtswirkungen zur Folge haben können, aber das Recht auf informationelle Selbstbestimmung kann davor schützen, Objekt einer allumfassenden Beobachtung zu werden, bei dem jede Regelüberschreitung staatlich registriert und mit Sanktionen belegt wird. Ohne Transparenz der Verwendungskontexte lässt sich auch das Ausmaß der Gefährdungen nicht überblicken, die mit einer Datenerhebung verknüpft sind.[69]

Umgekehrt kann eine besondere Engführung der Verwendungszwecke, die rechtlich und faktisch auch vor Zweckänderungen geschützt ist, die Gefährdungen u. U. soweit minimieren, dass eine Erhebung und Speicherung von Daten unterhalb der Schwelle eines Eingriffs in das Recht auf informationelle Selbstbestimmung verbleibt. So wird etwa in der Literatur die Speicherung von Ausleihdaten, die in einer Bibliothek anfallen, dann nicht für eingriffsrelevant erachtet, wenn die Stadtbücherei die Daten der ausgeliehenen Bücher lediglich zur Überwachung der Ausleihfristen nutzt und sicherstellt, dass die Daten nach der Rückgabe gelöscht werden, obwohl die Daten in anderen Kontexten ein besonders hohes Gefährdungspotenzial haben.[70] Dies dürfte freilich nur dann gelten, wenn auch eine Zweckänderung der Daten sowohl rechtlich als auch faktisch weitgehend ausgeschlossen ist.

3. Systemische Bewertung der Gefährdungen

Bereits auf der Eingriffsebene kommen auch Aspekte des systemischen Datenschutzes in den Blick. Die Datenerhebung, -speicherung und -verwendung kann so angelegt sein, dass bereits durch eine systemische Absicherung der Gefahren ein Grundrechtseingriff ausgeschlossen wird. So hat etwa auch das Bundesverfassungsgericht in seiner Entscheidung zur automatischen Kennzeichenerfassung in der bloß

69 G. Britz, Grundsatzkritik (Fn. 1), S. 584.

70 M. Germann, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000, S. 477 ff., Germann will die Eingriffsschwelle dort ansiedeln, wo die Behörde bei der Erhebung und Verwendung personenbezogener Daten den Kreis der konkret überschaubaren Verwendungszwecke überschreitet, ebd. S. 488 f. Vgl. auch M. Albers, Umgang (Fn. 1), Rn. 72.

maschinellen Speicherung der Fahrzeugdaten, deren automatische Löschung technisch gesichert ist, keinen Eingriff in das Recht auf informationelle Selbstbestimmung gesehen.[71]

Wird das Spezifikum des Schutzes des Kernbereichs der Persönlichkeitsentfaltung bei technisch unvermeidbaren Datenerhebungen und -speicherungen aus dem Kernbereich in dem Ausschluss jeglicher Verwertung gesehen,[72] so kann ein Auswertungssystem, dass das Verwertungsverbot – etwa durch eine unabhängige richterliche Kontrolle – sicherstellt und damit eine Verletzung der Menschenwürdegarantie ausschließt, ebenfalls als ein entsprechender systemischer Schutz – wenn auch nicht nur durch Technik – gesehen werden. Das Abstellen auf die Gefährdung der Grundrechtsentfaltung öffnet den Weg dafür, den Umgang mit personenbezogenen Daten systemisch so anzulegen, dass die eingriffsrelevante Gefährdungsschwelle nicht überschritten wird.

Dogmatischen Überlegungen zum Recht auf informationelle Selbstbestimmung, die bereits auf der Ebene des Grundrechtseingriffs ansetzen, ist entgegengehalten worden, dass sie allenfalls „äußerste Randbereiche" erfassen könnten.[73] Der Hinweis auf die Marginalität der bereits über den Eingriffsbegriff auszuschließenden Gefährdungen steht jedoch nicht in einem Gegensatz zu den vorstehenden Differenzierungen. Zum einen dürfen die Differenzierungen zum Eingriffsbegriff nicht dahin missverstanden werden, dass mit ihnen andere als marginale Gefährdungen aus dem Eingriffsbegriff ausgeschlossen werden sollen. Zum anderen sollen die Differenzierungen aber die Sensibilität dafür schärfen, dass die Marginalität von Gefährdungen gesellschaftlichen, technischen und epistemischen Veränderungen unterliegt und gerade auch von technischen Gestaltungen abhängig sein kann. Die Differenzierungen zum Eingriffsbegriff dienen dem Nachweis, dass ein Verständnis der informationellen Selbstbestimmung als reflexives Gefährdungsabwehrrecht auch in der Lage ist, die gesellschaftliche Dynamik der Marginalität abzubilden.

III. Grundrechtsgefährdung und Eingriffsrechtfertigung

Nur noch kurz angesprochen sei, dass das vorgeschlagene Verständnis der informationellen Selbstbestimmung als reflexives Gefährdungsabwehrrecht sich auch auf die Beurteilung der Rechtfertigung des Eingriffs auswirkt. Verbinden sich mit der Erhebung und Speicherung von Daten eingriffsrelevante Gefährdungen für die grundrechtliche Freiheitsentfaltung, so können diese Gefährdungen gerechtfertigt sein, wenn sie den allgemeinen und im Fall der Betroffenheit eines spezielleren Grundrechts den für dieses Grundrecht besonderen Rechtfertigungsanforderungen

71 BVerfGE 120, 378 (399); ähnlich BVerfGE 100, 313 (366); 107, 299 (328); 115, 320 (343).
72 Dazu R. Poscher, Menschenwürde und Kernbereichsschutz, JZ 2009, S. 269.
73 J. Masing, Gesetzesvorbehalt (Fn. 53), S. 476, 487 f.

genügen. Erst durch den Blick auf die Gefährdungen, die durch Informationseingriffe ausgelöst werden, wird es möglich, den Eingriff in das Recht auf informationelle Selbstbestimmung und die mit dem Eingriff verfolgten Ziele mit Blick auf den Verhältnismäßigkeitsgrundsatz zu relationieren. Mit den Gefährdungen sind auch diejenigen Interessen benannt, die im Rahmen einer in erster Linie vom Gesetzgeber zu gestaltenden Informationsordnung mit den Transparenz- und Informationsinteressen Dritter in ein Verhältnis gesetzt werden müssen.

Fast alle der im Zusammenhang mit der Beurteilung des Eingriffs aufgeführten Aspekte können jedenfalls im Rahmen der Verhältnismäßigkeit Bedeutung entfalten, wenn sich aus ihnen nicht bereits ergibt, dass bereits die Eingriffsschwelle nicht überschritten wurde. Dies gilt besonders für die Zweckbestimmung der Informationseingriffe, da sich bei Intransparenz der Verwendungszwecke nicht beurteilen lässt, welche Gefährdungen mit ihnen verbunden sind. Auch die systemische Betrachtung der Gefährdungen steuert nicht nur die Beurteilung des Ob eines Eingriffs, sondern auch die Beurteilung seiner Erforderlichkeit. Entsprechend betont das Urteil zur Vorratsdatenspeicherung die Absicherung von Datenbeständen auf dem Stand der Technik, um Missbrauchsgefahren zu minimieren.[74] Hier wird man aus grundrechtlicher Perspektive erwarten, dass die Behörden – aber auch die Geräte- und Softwareindustrie – im Hinblick auf die Absicherungen der Gefährdungen eine ähnliche Kreativität an den Tag legen, wie bei der Erschließung neuer Erhebungs- und Verwertungsmethoden.

D. Resümee

Die vorstehenden Überlegungen sollten eine mögliche Konzeption des Rechts auf informationelle Selbstbestimmung skizzieren. Sie konnten nicht auf alle Fragen eingehen, die sich für ein modernes Datenschutzgrundrecht stellen. So wurde etwa nicht auf Fragen der Drittwirkung eingegangen, die angesichts der weitgehenden Privatisierung der informationstechnischen Infrastruktur von besonderer Bedeutung sind. Insoweit sei hier nur darauf verwiesen, dass sich die Grundrechte als Abwehrrechte allgemein auch für eine Rekonstruktion der Drittwirkung fruchtbar machen lassen.[75] Auch auf die im Rahmen der Drittwirkung des Rechts auf informationelle Selbstbestimmung gefährdungsreduzierend und autonomieschonend wirkenden Möglichkeiten des zumutbaren Selbstschutzes wäre insoweit näher einzugehen. Trotz ihres insoweit fragmentarischen Charakters sollten die Überlegungen zur dogmatischen Struktur des Rechts auf informationelle Selbstbestimmung zeigen, dass es, verstanden als reflexives Abwehrrecht gegen Freiheitsgefährdungen durch die Erhebung, Speicherung und Verarbeitung von Daten, den wesentlichen Heraus-

74 BVerfGE 125, 260 (325 ff.).
75 R. Poscher, Grundrechte als Abwehrrechte, 2003.

forderungen gewachsen sein kann. Entgegen skeptischen Stimmen in der Literatur kann das so verstandene Grundrecht sowohl auf technische und gesellschaftliche Entwicklungen reagieren als auch auf die Kritik, die einen Abschied von dem Eingriffsabwehrrecht verlangt.[76]

Im Hinblick auf die Diskussion in den USA kann man Christopher Slobogin daher nur unterstützen. Es besteht kein Grund, sich durch die Diskussion in Deutschland irritieren zu lassen. Richtig verstanden, lässt sich das Recht auf informationelle Selbstbestimmung als ein sinnvolles subjektives Recht konstruieren, das allerdings gegenüber klassischen Grundrechten Besonderheiten aufweist. Das vorgeschlagene Verständnis der informationellen Selbstbestimmung als reflexives Recht zur Abwehr von Grundrechtsgefährdungen vermeidet eine sinnentleerte Verselbständigung des Rechts auf informationelle Selbstbestimmung und ist zukunftsoffen gegenüber technischen wie gesellschaftlichen Entwicklungen.

76 Vgl. auch G. Britz, Selbstdarstellung (Fn. 31), S. 84; dies., Grundsatzkritik (Fn. 1), S. 582 f., die zwar eher von einer Gewährleistungsstruktur des Grundrechts ausgeht, aber der Abwehrfunktion innerhalb dieser Struktur einen bedeutenden Stellenwert einräumt.

Data protection in European Law

Statement on
Prof. Slobogin "Is the 4th amendment relevant in a technological age?" and
Prof. Poscher "The future of the right to informational self-determination"

Jens-Peter Schneider

Both papers have presented extremely valuable insights into the complex national constitutional discussions of Germany and the US concerning security and privacy in the information society.

Prof. Slobogin demonstrated in his talk that strict preconditions for intrusions into privacy and strict remedies for illegal searches may look very effective in protecting privacy at a first glance, but they may also set strong incentives to restrict their applicability and thereby undermine their real effectiveness.

And Prof. Poscher showed that the judicial invention by our German constitutional court of a new fundamental freedom called informational self-determination may cause irritating conceptual uncertainties. Therefore, his presentation of an innovative reconceptualization is especially valuable.

To make our discussions even more complex I would like to draw your attention to the European constitutional framework which – first – is of obvious importance for transnational security networks in Europe and which – secondly – shows a great tendency to expand its applicability especially in the field of data protection.

The starting point of data protection in Europe has been the jurisprudence of the Strasbourg court on Art. 8 of the European Convention of Human Rights[1]. This article provides the right to respect for the private life of everyone. In contrast to the US example the ECHR construed this notion widely thereby protecting not only sensitive private data[2]. Besides, the Court gave room for a quite pluralistic balancing of conflicting interests under Art. 8 (2) ECHR[3]. In order to fulfil the requirement of

1 ECHR, 26.3.1987, appl. no. 9248/81 – Leander; 16.2.2000, appl. no. 27798/95 – Amann; 4.5.2000, appl. no. 28341/95 – Rotaru; 6.6.2006, appl. no. 62332/00 – Segerstedt-Wiberg; 4.12.2008, appl. no. 30562/04 et. Al. – Marper; see also ECHR, 12.1.2010, appl. no. 4158/05 – Gillan and Quinton on police search competences; for a systematic overview see: Birte Siemen, Datenschutz als europäisches Grundrecht, Berlin 2006, pp. 51-211; see also Marion Albers, Informationelle Selbstbestimmung, Baden-Baden 2005, pp. 290-297.

2 ECHR, 16.2.2000, appl. no. 27798/95 – Amann, para. 44, 65 et seqq.; 4.5.2000, appl. no. 28341/95 – Rotaru, para 42 et seqq.; 6.6.2006, appl. no. 62332/00 – Segerstedt-Wiberg, para 71-72; 4.12.2008, appl. no. 30562/04 et. Al. – Marper, para 66 et seqq.; see also ECHR, 12.1.2010, appl. no. 4158/05 – Gillan and Quinton, para 61 et seqq.

3 ECHR, 26.3.1987, appl. no. 9248/81 – Leander, para. 58 et seqq.; 16.2.2000, appl. no. 27798/95 – Amann; 4.5.2000, appl. no. 28341/95 – Rotaru, para 47; 6.6.2006, appl. no. 62332/00 – Segerstedt-Wiberg, para 87 et seqq.; 4.12.2008, appl. no. 30562/04 et. Al. – Marper, para 100.