Das Recht auf informationelle Selbstbestimmung

Von Dr. **Claudio Franzius**, Berlin/Hamburg*

Die Ankündigung des Bundesjustizministers für ein neues Gesetz zur Einführung der umstrittenen Vorratsdatenspeicherung wirft Fragen nach den verfassungsrechtlichen Grenzen auf, die vor allem durch Art. 10 GG gezogen werden. Grundlegend für den Datenschutz in Deutschland ist jedoch das Recht auf informationelle Selbstbestimmung. Was verbirgt sich hinter diesem Grundrecht und wie sollte es gedacht werden? Der Datenschutz ist längst vor internationale Herausforderungen gestellt, die Lösungen nicht mehr allein vom nationalen Recht erwarten lassen.

I. Einführung

Das Recht auf informationelle Selbstbestimmung bildet eine zentrale Grundlage für den Datenschutz in Deutschland. Es wurzelt im berühmten Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983 (II.). Vorliegend wird die Struktur des Grundrechts erläutert und gezeigt, dass sich die Rechtsprechung um Kontinuität bemüht (III.). Das gilt trotz der Kritik an der Vorstellung einer eigentumsanalogen Verfügungsbefugnis über die „eigenen" Daten und der hierdurch erzwungenen Verrechtlichung, der nur begrenzte Steuerungsleistungen korrespondieren (IV.). Für eine Neukonzeption des Rechts auf informationelle Selbstbestimmung lassen sich drei Strategien unterscheiden, die in den Kontext der überstaatlichen Herausforderungen des Datenschutzes gestellt werden (V.).

II. Grundlegung

Das BVerfG hat im Volkszählungsurteil das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts vor dem Hintergrund der „heutigen und künftigen Bedingungen der automatischen Datenverarbeitung" anerkannt.[1] Dieses Grundrecht sichert dem Einzelnen die Befugnis, grundsätzlich „selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" und „zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden." Zudem müssen Betroffene „wissen können, wer was wann und bei welcher Gelegenheit über sie weiß". Für die Rechtfertigung des Eingriffs in das Recht auf informationelle Selbstbestimmung, das Eingang in viele Landesverfassungen[2] gefunden hat, statuiert das Gericht strenge Anforderungen: Jede Beschränkung des Rechts auf informationelle Selbstbestimmung bedarf einer verfassungsmäßigen gesetzlichen Grundlage, die aus Gründen des überwiegenden Allgemeininteresses zulässig und erforderlich sein sowie dem Gebot der Normenklarheit und dem Grundsatz der Verhältnismäßigkeit entsprechen muss.

1. Schutzgegenstand

Ausgangspunkt ist das verfassungsrechtliche Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Im Kern geht es um eine Fortentwicklung des Rechts auf Achtung der Privatsphäre, wobei als Schutzgegenstand die Selbstbestimmung des Einzelnen und als Gefährdungslage der konkrete Verwendungszusammenhang von Daten ausgemacht wurde. Weil die sozialen Bezüge und Verwendungszusammenhänge aber nicht zum Gegenstand des Schutzbereichs erklärt, sondern bei den Schranken verortet werden, *verselbständigte* sich das Recht auf informationelle Selbstbestimmung und ließ den grundrechtlichen Freiheitsvoraussetzungsschutz zum Inhalt eines Grundrechts werden.[3] Deshalb sind die eingriffsabwehrrechtlichen Konturen des Rechts auf informationelle Selbstbestimmung unscharf geblieben.[4]

Nach der ständigen Rechtsprechung des BVerfG ist der Schutzbereich durch die Befugnis des Einzelnen gekennzeichnet, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[5] Schutzgegenstand ist eine Datenverfügungsbefugnis, die zwar nicht unmittelbar das grundrechtliche Schutzgut abbildet und damit nicht um ihrer selbst willen geschützt ist, dessen abwehrrechtlicher Schutz dann aber schnell auf einen Mechanismus zur Sicherung anderer Freiheiten verkürzt wird.[6] Hält man demgegenüber an einem eigenständigen „Schutzbereich" fest, so fragt sich, ob seine Kennzeichnung als eigentumsanaloges Informationsbeherrschungsrecht angemessen ist. Während das allgemeine Persönlichkeitsrecht heute jedenfalls insoweit eine zurückhaltendere Schutzbereichsbestimmung erhält als Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG kein allgemeines und umfassendes (!) Verfügungsrecht über die Darstellung der eigenen Person[7] zu entnehmen ist, der soziale Kontext vielmehr an Bedeutung gewinnt, ist das beim Recht auf informationelle Selbstbestimmung bislang nur begrenzt der Fall und die Argumentationslast verlagert sich auf die Rechtfertigungsebene. Obwohl der Datenschutz kontextspezifisch auch

---

* Der *Verf.* ist Privatdozent an der Juristischen Fakultät der Humboldt-Universität zu Berlin.

[1] BVerfGE 65, 1 (42). Grundlegend zuvor *Podlech*, in: Perels (Hrsg.), Grundrechte als Fundament der Demokratie, 1979, S. 50. Zur Rekonstruktion *Steinmüller*, RDV 2007, 158.

[2] Art. 33 BerlVerf; Art. 11 BrandenbVerf; Art. 12 Abs. 3-5 BremVerf; Art. 6 Abs. 1-2 MVVerf; Art. 4 Abs. 2 NWVerf; Art. 4a RPVerf; Art. 2 S. 2 SaarVerf; Art. 6 Abs. 1 SachsAnhVerf; Art. 6 Abs. 2-4 ThürVerf.

[3] *Bull*, ZRP 1998, 310 (312); *Ladeur*, DuD 2000, 12; *Trute*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 2 Rn. 11 („ersichtlich zu weit").

[4] Krit. *Ladeur*, DÖV 2009, 45. Der Freiheitsbegriff des Grundgesetzes erschöpft sich nicht in der Ausgrenzung eines Raums eigenen Beliebens, sondern meint rechtlich geordnete Freiheit, vgl. *Schmidt-Aßmann*, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. 2, 3. Aufl. 2004, § 26 Rn. 31. Gegen die Verkürzung auf die Staatsabwehrdoktrin auch *Hoffmann-Riem*, AöR 123 (1998), 513 (523 ff.).

[5] BVerfGE 65, 1 (42 f.); 118, 168 (184); 120, 274 (312).

[6] So *Britz*, in: Hoffmann-Riem, Offene Rechtswissenschaft, 2010, S. 561 (582).

[7] BVerfGE 101, 361 (380); 120, 180 (198).

in den speziellen Freiheitsgarantien verortet und der Schutzbereich des informationellen Selbstbestimmungsrechts für neue Inhalte geöffnet wird, bleibt dieser isoliert auf einzelne Daten ausgerichtet und der maßgebliche Bezugspunkt der Information wird erst auf der Ebene der Eingriffsrechtfertigung im Rahmen der Abwägung relevant.[8]

2. Eingriffsrechtfertigungen

Unter Zugrundlegung eines weiten Eingriffsbegriffs, der nicht immer erkennen lässt, welcher Schritt der Datenerhebung und -verarbeitung als rechtsrelevante Aktion herauszukristallieren und damit als Eingriff zu qualifizieren ist, kommt es entscheidend auf die verfassungsrechtliche Rechtfertigung an. Das BVerfG hat den Schrankenvorbehalt des Art. 2 Abs. 1 GG für das Recht auf informationelle Selbstbestimmung präzisiert:

Maßgeblich sind die Grundsätze der Bestimmtheit und Normenklarheit. Der Gesetzgeber habe Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen. Bediene sich der Gesetzgeber unbestimmter Rechtsbegriffe, dürfen verbleibende Ungewissheiten nicht so weit gehen, dass die Vorhersehbarkeit und Justiziabilität des Handelns der durch die Normen ermächtigten staatlichen Stellen gefährdet sind.[9] Erst allmählich wird klar, dass hier ein Spannungsverhältnis besteht: Je bestimmter die Norm bereichsspezifisch zu fassen ist, desto weniger normenklar werden die Anforderungen des Datenschutzes für den Einzelnen.[10]

Herausragende Bedeutung wird dem Grundsatz der Zweckbindung zugesprochen: Das eingriffsrechtfertigende Gesetz muss eine Bestimmung über die Zweckbindung enthalten, wonach gewonnene Daten nur zu den Zwecken verwendet werden dürfen, zu denen sie erhoben wurden. Auch diese Konditionalprogrammierung scheint der Realität, wozu das anlasslose Sammeln von Daten durch private Unternehmen gehört, nur noch begrenzt gerecht werden zu können. Zwar geht das BVerfG davon aus, dass eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder nicht bestimmbaren Zwecken verfassungswidrig wäre. Diesem Verbot unterfalle eine vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung und Verwertung jedoch nicht.[11]

Das Gesetz muss auch den verfassungsrechtlichen Maßgaben zum Schutz des Kernbereichs gerecht werden. Heimliche Überwachungsmaßnahmen staatlicher Stellen haben den unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt.[12] Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen.[13] Um diesen Vorgaben gerecht zu werden, sind Schutzkonzepte häufig zweistufig ausgestaltet. Auf der ersten Stufe hat eine gesetzliche Ermächtigung so weit wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden. Bei heimlichen Zugriffen ist es jedoch praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann. Daher muss auf der zweiten Stufe für hinreichenden Schutz in der Auswertungsphase gesorgt sein. Insbesondere müssen aufgefundene und erhobene Daten mit Kernbereichsbezug unverzüglich gelöscht und ihre Verwertung ausgeschlossen werden.[14]

In der eingriffsabwehrrechtlichen Konstruktion des BVerfG spielt der Grundsatz der Verhältnismäßigkeit eine zentrale Rolle. Danach wird verlangt, dass der Grundrechtseingriff einem legitimen Zweck dient und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen ist. Grundsätzlich dürfte gegenüber dem heimlichen Zugriff eine offene Erhebung das mildere Mittel sein. Der Gesetzgeber hält aber häufig nur die verdeckte Erhebung der Daten für erfolgversprechend, so dass die Argumentationslast in die Angemessenheitsprüfung verlagert wird. Hier darf die Schwere des Eingriffs nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen.[15] Der Gesetzgeber hat das Individualinteresse, das durch einen Grundrechtseingriff beschnitten wird, den Allgemeininteressen, denen der Eingriff dient, angemessen zuzuordnen. Die Prüfung an diesem Maßstab kann ergeben, dass ein Mittel nicht zur Durchsetzung von Allgemeininteressen angewandt werden darf, weil die davon ausgehenden Grundrechtsbeeinträchtigungen schwerer wiegen als die durchzusetzenden Belange.[16]

III. Beispiele aus der Rechtsprechung

1. BVerfGE 65, 1 (Volkszählung)

Die Besonderheit des Rechts auf informationelle Selbstbestimmung liegt weniger darin, dass hier ein neues Grundrecht „erfunden" wurde, sondern im Zusammenziehen mehrerer Argumentationsstränge aus der Rechtsprechung des Gerichts, das schon in der Mikrozensus-Entscheidung unter Rückgriff auf seine Menschenwürde-Rechtsprechung dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung zugewiesen hat, der Einwirkungen der öffentlichen

[8] Näher *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 2. Aufl. 2012, § 22 Rn. 68; *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 17 ff.

[9] BVerfGE 120, 274 (315 f.).

[10] Vgl. *Kingreen/Kühling*, JZ 2015, 213 (215 f.).

[11] BVerfGE 125, 260 (316); schärfer EuGH, Urt. v. 8.4.2014 – C-293/12 und C-514/12 (Digital Rights Ireland u.a.). Zu den Unterschieden *Spiecker gen. Döhmann*, JZ 2014, 1109 (1113).

[12] BVerfGE 6, 32 (41); 27, 1 (6); 32, 373 (378); 34, 238 (245); 80, 367 (373); 109, 279 (313); 113, 348 (390).

[13] BVerfGE 109, 279 (314).

[14] BVerfGE 109, 279 (318); 113, 348 (391 f.).

[15] Vgl. BVerfGE 90, 145 (173); 109, 279 (349 ff.); 113, 348 (382).

[16] BVerfGE 120, 274 (321 f.). Für ein Beispiel OVG Hamburg, NJW 2008, 96.

Gewalt entzogen sein soll.[17] In den Schutzbereich des informationellen Selbstbestimmungsrechts fließen Elemente der Rechtsprechung zum allgemeinen Persönlichkeitsrecht, der Selbstbestimmung im Sinne einer Bestimmungsbefugnis über die „eigenen" Daten und die Sicherung der Verhaltensfreiheit „im Hinblick auf Unwissenheit über das Wisser Anderer über die eigene Person."[18] Aber nicht bloß den Bezug zur Verhaltensfreiheit stellt das Gericht heraus, wenn es ausführt:

„Individuelle Selbstbestimmung setzt [...] voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten [...]. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichenden Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."[19]

Obwohl Selbstbestimmung nicht bloß individuell verstanden, sondern auf das kollektive Gemeinwesen bezogen wird und die freie Entfaltung der Persönlichkeit unter den Bedingungen der Datenverarbeitung *deshalb* den Schutz des Einzelnen gegen die unbegrenzte Erhebung, Speicherung und Verwendung „seiner" persönlichen Daten verlange, konstruiert das BVerfG das Recht auf informationelle Selbstbestimmung als Eingriffsabwehrrecht und hält daran bis heute fest.[20] Das mag der damals als neu empfundenen Gefährdung durch staatlich eingesetzte Großrechenanlagen geschuldet gewesen sein, erweist sich aber angesichts der neuen Gefährdungen durch private Akteure wie Facebook, Google oder andere Internetdienste als prekär, passt die Figur der Eingriffsabwehr doch grundrechtsdogmatisch für Privatrechtsbeziehungen nicht. Der genetische Code des Rechts auf informationelle Selbstbestimmung liegt in der bipolaren Konstellation eines für übermächtig gehaltenen Staates, dem die um individuelle „Selbstbestimmung" angereicherte Handlungsfreiheit der Bürger einfach gegenübergestellt wird. Bis heute hat das BVerfG eine überzeugende Antwort auf die verfassungsrechtlichen Fragen des Datenschutzes im Privatrecht nicht gefunden.[21] Zwar liegt mit der Figur der Schutzpflichten ein grundrechtsdogmatischer „Aufhänger" bereit. Daraus folgt jedoch kein strikter Gesetzesvorbehalt für private Datenverarbeitungsvorgänge, sondern im Grunde nur, dass ein rechtlicher Rahmen zur tatsächlichen Sicherung des informationellen Selbstschutzes bereitgestellt wird.[22]

2. BVerfGE 120, 378 (Kfz-Kennzeichenerfassung)

In einer Reihe von Entscheidungen hat das BVerfG den Gesetzesvorbehalt zum Anlass genommen, die Verantwortung des Gesetzgebers für die differenzierte Strukturierung von Datenverarbeitungsvorgängen hervorzuheben.[23] Dass es, wie es im Volkszählungsurteil heißt, kein „belangloses" Datum geben kann, wird dahingehend präzisiert, dass es auf den Verwendungskontext ankommt.[24] Hierdurch wird unterstrichen, dass personenbezogene Daten erst in bestimmten Kontexten zur Information werden und je nach Kontext eine völlig neue Bedeutung erhalten können.[25]

Das Recht auf informationelle Selbstbestimmung, wie es namentlich im informationsbezogenen Polizeirecht seinen Niederschlag gefunden hat, erweitert den grundrechtlichen Schutz von Verhaltensfreiheit, indem es ihn schon auf der

---

[17] BVerfGE 27, 1 (6) mit Bezugnahme auf BVerfGE 6, 32 (41); 6, 389 (433).

[18] *Trute* (Fn. 3), Kap. 2 Rn. 9. Zur Rekombination der Stränge aus verschiedenen Zusammenhängen in der eingriffsabwehrrechtlichen Verbürgung eines Entscheidungsrechts über die Preisgabe und Verwendung persönlicher Daten *Albers* (Fn. 8), § 22 Rn. 61.

[19] BVerfGE 65, 1 (42 f.), *Hervorhebungen* des *Verf.*

[20] Krit. *Albers*, in: Haratsch/Kugelmann/Repkewitz (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft, 1996, S. 113. Zum „Sprung in der Argumentation" auch *Trute* (Fn. 3), Kap. 2 Rn. 9 mit Fn. 40; *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl. 2011, S. 33 f. Danach ist es eine Sache, dass die Sammlung und Verwendung von Informationen über Individuen nicht unbegrenzt erlaubt sein kann, die daraus entwickelte Schlussfolgerung, der Einzelne müsse grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen, aber keineswegs zwingend.

[21] Vgl. *Bäcker*, Der Staat 51 (2012), 91 (97 ff.).

[22] BVerfG, Beschl. v. 17.7.2013 – 1 BvR 3167/08 = NJW 2013, 3086.

[23] Vgl. *Bull*, in: van Ooyen/Möllers (Hrsg.), Handbuch Bundesverfassungsgericht im politischen System, 2. Aufl. 2015, S. 627.

[24] BVerfGE 120, 378 (399). Das war in BVerfGE 65, 1 (45) undeutlich geblieben.

[25] Deshalb kann die Begrenzung der Verwendung eine Speicherung rechtfertigen, vgl. mit Blick auf die Speicherung und anschließender Übermittlung von personenbezogenen Telekommunikationsdaten BVerfGE 125, 260 (327 f.): „Eine Speicherung von Telekommunikationsverkehrsdaten [...] setzt gesetzliche Regelungen zur Verwendung dieser Daten voraus. Die verhältnismäßige Ausgestaltung dieser Verwendungsregeln entscheidet damit nicht nur über die Verfassungsmäßigkeit dieses einen eigenen Eingriff begründenden Bestimmungen selbst, sondern wirkt auf die Verfassungsmäßigkeit schon der Speicherung als solcher zurück." Hieran kann ungeachtet aller Zweifelsfragen eine neue Regelung der Vorratsdatenspeicherung anknüpfen.

Stufe der Persönlichkeitsgefährdung beginnen lässt. Hier hat es den Anschein, als werde der Verzicht auf einen konkreten Nachteilsbezug[26] durch den Hinweis auf die fehlende Benennbarkeit konkret bedrohter Rechtsgüter kompensiert. Es kommt zu einem in das Vorfeld verlagerten Gefährdungsschutz. Einer vollständigen Entkoppelung von möglichen Rechtsgutverletzungen wird dadurch vorgebeugt, dass eine *besondere Gefährdungslage* verlangt wird.[27]

Das Urteil verdeutlicht die abwehrrechtliche Konstruktion des informationellen Selbstbestimmungsrechts und macht die Anforderungen des Gesetzesvorbehalts hinsichtlich der Bestimmtheit der gesetzlichen Grundlage von der Intensität des Eingriffs abhängig, die durch das Zweckbindungserfordernis abgemildert wird. Weil die Anforderungen an die Zweckfestlegung der Minderung der Eingriffsintensität und nur mittelbar der Sicherung der Parlamentsverantwortung dienen, könne die Festlegung auch administrativ erfolgen.[28] Auch der Auskunftsanspruch sowie allgemein die Einräumung von Kenntnis- und Einflussrechten der Betroffenen können gerade bei heimlicher Datenverarbeitung aus Verhältnismäßigkeitsgesichtspunkten geboten sein. Das mildert den so genannten chilling effect, aus Sorge vor einer Speicherung abweichender Verhaltensweisen durch solche Verhaltensweisen seine Grundrechte in Anspruch zu nehmen.[29]

In jüngeren Entscheidungen hat das BVerfG diesen Einschüchterungseffekt hervorgehoben.[30] So vermittelt dem Gericht zufolge die automatische Erfassung von Kfz-Kennzeichen die Eindruck ständiger Kontrolle. Das „sich einstellende Gefühl des Überwachtwerdens“ könne zu Einschüchterungseffekten und in der Folge zu Beeinträchtigungen bei der Ausübung von Grundrechten führen. Dadurch seien nicht nur die individuellen Entfaltungschancen des Einzelnen betroffen, sondern auch das Gemeinwohl, weil „die Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen Gemeinwesens“ ist.[31] Dass es hierbei nicht allein um deutsche Befindlichkeiten geht, wir es also mit keiner querelle d’ allemand zu tun haben, dokumentiert das Urteil des EuGH zur Grundrechtswidrigkeit der Vorratsdatenspeicherungsrichtlinie, das nach den Schlussanträgen von Generalanwalt *Pedro Cruz-Villalón*[32] explizit auf Ausführungen des BVerfG zum Einschüchterungseffekt der Vorratsdatenspeicherung[33] Bezug nimmt.[34]

3. BVerfGE 120, 274 (Online-Durchsuchung)

In seinem Urteil zur heimlichen Infiltration privater Computer hat das BVerfG die Grenzen seiner Konzeption des grundrechtlichen Datenschutzes erkannt und einer „Überfrachtung“ des Rechts auf informationelle Selbstbestimmung vorzubeugen versucht. Werde ein informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert, so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt *auszuspähen*.

Das BVerfG arbeitet heraus, dass den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit weder durch Art. 10 Abs. 1 GG noch durch Art. 13 Abs. 1 GG hinreichend begegnet werden könne. Danach schützt Art. 10 GG die laufende, nicht aber die abgeschlossene Kommunikation. Art. 13 GG schütze nur die räumliche Privatsphäre, nicht aber die Infiltration eines PC außerhalb der Wohnung. Auch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf Schutz der Privatsphäre reiche nicht aus, um angemessenen Schutz zu gewährleisten:

„In seiner Ausprägung als Schutz der Privatsphäre gewährleistet das allgemeine Persönlichkeitsrecht dem Einzelnen einen räumlich und thematisch bestimmten Bereich, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll […]. Das Schutzbedürfnis des Nutzers eines informationstechnischen Systems beschränkt sich jedoch nicht allein auf Daten, die seiner Privatsphäre zuzuordnen sind. Eine solche Zuordnung hängt zudem häufig von dem Kontext ab, in dem die Daten entstanden sind und in den sie durch Verknüpfung mit anderen Daten gebracht werden. Dem Datum selbst ist vielfach nicht anzusehen, welche Bedeutung es für den Betroffenen hat und welche es durch Einbeziehung in andere Zusammenhänge gewinnen kann. Das hat zur Folge, dass mit der Infiltration des Systems nicht nur zwangsläufig private Daten erfasst werden, sondern der Zugriff auf alle Daten ermöglicht wird, so dass sich ein umfassendes Bild vom Nutzer des Systems ergeben kann.“[35]

Weil das Recht auf informationelle Selbstbestimmung auf punktuelle Datenerhebungen ausgelegt ist, biete es keinen ausreichenden Schutz vor den Gefahren, die durch die Nutzung informationstechnischer Systeme bedingt sind. Wer informationstechnische Systeme nutzt, ist gezwungen, dem System persönliche Daten zu liefern. Werde auf dieses System zugegriffen, verfüge der Zugreifende auf Anhieb über einen potenziell großen und aussagekräftigen Datenbestand und sei auf weitere Datenerhebungs- oder Datenverarbeitungsmaßnahmen nicht mehr angewiesen. Insofern bestehe bei Anwendung des Rechts auf informationelle Selbstbestimmung eine Schutzlücke. Diese Lücke schloss das BVerfG in der Entscheidung zur Online-Durchsuchung, indem es das

[26] Krit. *Bull* (Fn. 20), S. 92.
[27] Vgl. *Britz* (Fn. 6), S. 578 ff.
[28] Vgl. *Britz* (Fn. 6), S. 584.
[29] Siehe auch *Masing*, in: Hoffmann-Riem, Offene Rechtswissenschaft, 2010, S. 467 (490): „Besteht die Gefahr, dass jede Abweichung vom common sense festgehalten wird, entsteht ein Anpassungsdruck, der individuell Zivilcourage hemmen und gesellschaftlich die Innovationskraft der Freiheit konterkarieren kann.“
[30] BVerfGE 113, 29 (46 f.); 115, 166 (188); 120, 378 (402); krit. *Bull* (Fn. 23), S. 641 ff.
[31] BVerfGE 120, 378 (430); krit. *Nettesheim*, VVDStRL 70 (2011), 7 (28 f.); *Bull* (Fn. 20), S. 63 ff.
[32] EuGH (Generalanwalt *Cruz-Villalón*), Schlussanträge v. 12.12.2013 – C-293/12 und C-514/12 (Digital Rights Ireland u.a.), Rn. 52, 72.
[33] BVerfGE 125, 260 (320); anders die abw. Meinung des Richters *Eichberger*, BVerfGE 125, 364 (366).
[34] EuGH, Urt. v. 8.4.2014 – C-293/12 und C-514/12 (Digital Rights Ireland u.a.), Rn. 37.
[35] BVerfGE 120, 274 (311 f.).

Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG entwickelt:

„Soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist, trägt das allgemeine Persönlichkeitsrecht dem Schutzbedarf in seiner lückenfüllenden Funktion über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung, dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet. Dieses Recht fußt gleich dem Recht auf informationelle Selbstbestimmung auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Es bewahrt den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten."[36]

Dieses, mitunter missverständlich als Computer-Grundrecht bezeichnete Recht schützt das Interesse des Nutzers, dass die von einem informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Erkennbar stellt das Gericht auf die Systemanforderungen ab und spezifiziert die Angemessenheitsprüfung. Der gesetzlich geregelte Eingriffsanlass muss nach Rang und Art der Gefährdung der Schutzgüter ein hinreichendes Gewicht aufweisen. Online-Durchsuchungen dürfen nur zum Schutze überragend wichtiger Rechtsgüter erfolgen. Das können der Bestand oder die Sicherheit des Bundes oder Landes, die Integrität von Leib, Leben und Freiheit oder schwere Straftaten sein. Was jedoch ein „informationstechnisches System" ist und wie „Vertraulichkeit" oder „Integrität" zu bestimmen sind, bleibt nach der Entscheidung des BVerfG unsicher und hat im Schrifttum zur Kritik geführt.[37] Trotz dieser offenen Fragen besteht eine Leistung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme darin, dass nunmehr auch in der Rechtsprechung des BVerfG deutlich wird, mit einem auf Entscheidungsbefugnisse des Einzelnen fokussierten Schutzkonzept nicht immer weiter zu kommen.[38]

IV. Kritik und Neukonzeption

Seit Jahren richtet sich die konzeptionelle Kritik am Recht auf informationelle Selbstbestimmung auf die Konstruktion einer eigentumsanalogen Befugnis an etwas, was nur als sozialer Vorgang angemessen begriffen werden könne. Der vom BVerfG garantierte Schutz der Grundrechtsträger erfordert das Mitdenken von Kontexten und die Berücksichtigung kontextual gefasster mehrdimensionaler Grundrechtspositionen. Deshalb fokussiert die Kritik auf die abwehrrechtliche Konstruktion des Grundrechts, womit weder neue Gefährdungen durch private Unternehmen angemessen in den Griff zu bekommen sind noch die maßgebliche Grundrechtsfunktion für die Ausgestaltung des einfachen Rechts benannt ist.

1. Eigentumsanaloge Verfügungsbefugnis

Zwar hat das BVerfG schon im Volkszählungsurteil die soziale Dimension von Informationsvorgängen herausgestellt. Der Einzelne habe kein Recht im Sinne einer absoluten, uneingeschränkten Herrschaft über „seine" Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stelle kein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Allerdings hat das Gericht die soziale Dimension von Informationsverarbeitungsvorgängen grundrechtsdogmatisch nicht im Schutzbereich des Rechts auf informationelle Selbstbestimmung verortet, sondern als Problem kollidierender Rechte in der Schrankendogmatik verarbeitet. Damit erscheint das informationelle Selbstbestimmungsrecht als eine absolute Verfügungsbefugnis, die wie andere Grundrechte zugunsten anderer Rechte gegebenenfalls zurückstehen muss.

Ein so weiter Schutzbereich ist aber schlecht zu begründen. Eigentumsanaloge Informationsbeherrschungsrechte, die ein Recht auf das „Haben" von Informationen beeinhalten würden, liefen darauf hinaus, dem Einzelnen ein Recht an Beobachtungen und Sinnkonstruktionen anderer zuzuweisen.[39] Das kann schon vor dem Hintergrund der anderen Grundrechtspositionen nicht sein[40] und vernachlässigt den sozialen Kontext, in den Informationen gestellt sind, ja dadurch überhaupt erst zu einer Information werden. Das muss keinen Abschied vom grundrechtlichen Datenschutz bedeuten. Die Vielfalt der Schutz- und Ordnungsbedürfnisse kann von der Grundrechtsdogmatik dadurch verarbeitet werden, dass Gewährleistungsgehalte mit Hilfe überindividueller Perspektiven formuliert werden.

2. Verrechtlichung ohne Steuerungsleistungen

Inzwischen wird immer klarer, dass die Konzeption des BVerfG mit der Fokussierung auf die Eingriffsabwehr an Grenzen stößt und der reale Gewinn an Freiheitsschutz durchaus bestritten werden kann. Konzentriert man die Fragen des Datenschutzes auf die abwehrrechtlichen Gehalte der Grundrechte, liegen die Folgen auf der Hand, mögen sie mitunter auch zu drastisch beschrieben werden. Es droht eine Verrechtlichung, weil der Eingriff in den „Schutzbereich" des Rechts auf informationelle Selbstbestimmung den Gesetzes-

[36] BVerfGE 120, 274 (313).

[37] Statt vieler *Britz*, DÖV 2008, 411 (413 ff.); *Eifert*, NVwZ 2008, 521 (522 ff.).

[38] Zum objektiv-rechtlichen Rahmen des subjektiven Rechts auf „Gewährleistung" der Integrität und Vertraulichkeit informationstechnischer Systeme *Hoffmann-Riem*, JZ 2014, 53 (57); siehe auch *Ladeur*, DÖV 2009, 45 (54 f.).

[39] Vgl. *Trute* (Fn. 3), Kap. 2 Rn. 19; *Albers*, Rechtstheorie 33 (2002), 61 (81).

[40] Das kulminiert in der Feststellung, eine unmittelbar an die individuelle Verfügungsbefugnis anknüpfende Konzeption gewähre Unmögliches (Informationsverfügungsbefugnis) oder normativ nicht Erforderliches (Datenverfügungsbefugnis), vgl. *Britz* (Fn. 6), S. 567 f.

vorbehalt auslöst.[41] Ein Blick in die Standardbefugnisse des Polizei- und Ordnungsrechts veranschaulicht den Zuwachs an rechtlichen Regelungen zur Legitimierung des informationsbezogenen Handelns der Polizei und Ordnungsbehörden. Das Bestimmtheitserfordernis für die Rechtfertigung von Eingriffen in das Recht auf informationelle Selbstbestimmung tritt in ein Spannungsverhältnis zur Normenklarheit, ist es den Betroffenen angesichts der verstreuten Regeln im Bundesdatenschutzgesetz und der Zunahme an bereichsspezifischen Regelungen in sachgebietsbezogenen Gesetzen doch kaum noch möglich, die Anforderungen für die Erhebung, Verwertung und Weitergabe von Daten zu erkennen.

Mit anderen Worten: Es droht nicht bloß eine Verrechtlichungsfalle.[42] Angesichts des sich schnell verändernden technischen, sozialen und wirtschaftlichen Kontexts laufen die Regelungen des Datenschutzes auch Gefahr, ihre Steuerungskraft einzubüßen. Mehr Recht bedeutet nicht stets bessere Steuerungsfähigkeit.[43] Obwohl eine Stärke des Datenschutzes in der Einbeziehung des sozialen Umfelds gesehen werden konnte, droht das Recht auf informationelle Selbstbestimmung an der Realität aufzulaufen, soweit es nicht gelingt, den wachsenden Differenzierungsbedarf grundrechtlich aufzufangen. Statt Forderungen nach dem einen Grundrecht auf Datenschutz nachzugeben, wird man dem Charakter des Datenschutzrechts als Querschnittsmaterie auch grundrechtsdogmatisch zu entsprechen haben. Die Aufgabe der Wissenschaft liegt darin, die Beharrungskräfte der Rechtsprechung auf ihre Stimmigkeit zu überprüfen, die Folgen zu überdenken und Neukonzeptionen in die Diskussion über das eigentümliche Recht auf informationelle Selbstbestimmung einzuspeisen.

3. Ansätze einer Neukonzeption

Wie aber sehen solche Neukonzeptionen aus? Im Wesentlichen lassen sich heute drei Strategien unterscheiden. Sie haben unterschiedliche Implikationen für die Rolle des Rechts auf informationelle Selbstbestimmung und den Datenschutz.

a) Reduzierung auf Missbrauchsschutz?

Die erste Option wäre eine „Abrüstung" verfassungsrechtlicher Vorgaben.[44] Den Mittelpunkt der Kritik bildet die „Überdehnung" des Rechts auf informationelle Selbstbestimmung, dessen Erstreckung in den öffentlichen Raum über den Schutz der Privatsphäre hinausgehe.[45] Werde wegen der großen „Streubreite" einer Maßnahme und schon wegen des bloßen „Gefühls" des Überwachtwerdens ein Eingriff mit erheblichem Gewicht bejaht, gingen die Konturen des Eingriffsabwehrrechts verloren. Vorgeschlagen wird kein Umbau der Konzeption, aber eine Rückbesinnung auf die Schutzgüter der Privatheit und Verhaltensfreiheit mit der Abwehr von Gefährdungen und Verletzungen der Persönlichkeit.[46] Auch der extrem weite Eingriffsbegriff, der die „Illusion" zur Grundrechtskategorie erhebe und bereits „ein Gefühl des Überwachtwerdens" den Eingriff indizieren lasse, müsse überdacht werden.[47] Die notwendige Konturierung des Schutzbereichs könne nur durch eine stärkere Rückkoppelung des Rechts auf informationelle Selbstbestimmung an das allgemeine Persönlichkeitsrecht zurückgewonnen werden und der Eingriffsbegriff bedürfe der Revision, weil anderenfalls nahezu jeder staatliche Umgang mit personenbezogenen Daten ohne oder gegen den Willen des Betroffenen als Eingriff qualifiziert werden müsse und damit dem Vorbehalt des Gesetzes unterstellt wäre.[48]

Die Folge wäre ein enges Verständnis des Datenschutzrechts ohne größere Auswirkungen auf die Informationsordnung. Deren Ausgestaltungsvorgaben müssen dann aus anderen Grundrechten entwickelt werden, wofür das Persönlichkeitsrecht mit dem Schutz der Privatsphäre einen konzeptionell begrenzten Ansatz liefern würde. Auch der EuGH hat sein grundlegendes Datenschutz-Urteil in der Rechtssache Google Spain[49] im Wesentlichen auf Art. 7 GRCh mit dem Schutz der Privatsphäre gestützt, obwohl der Datenschutz in Art. 8 GRCh eine eigene grundrechtliche Absicherung gefunden hat. Es kann nach der Rechtsprechung des BVerfG aber nicht allein auf die Sphären des abgestuften Persönlichkeitsschutzes (Intim-, Privat- und Sozial- bzw. Öffentlichkeitssphäre) ankommen. Vielmehr sind die unterschiedlichen Verwendungskontexte mit dem jeweiligen Gefährdungspotential in den Blick zu nehmen.[50] Eben das vermag die Aufspaltung des Schutzes in speziell normierte Freiheitsrechte einerseits und die am „Sphärenschutz" anknüpfende Persönlichkeitsentfaltung andererseits nur begrenzt zu leisten. Dies umso mehr, wenn auf eine ex ante Steuerung der Verwen-

[41] Zur Rationalität dieses Vorgehens vgl. *Masing* (Fn. 29), S. 487 ff.

[42] Von der „Verrechtlichung des Alltäglichen" spricht *Hoffmann-Riem*, AöR 123 (1998), 513, (527 f.); *Bull* (Fn. 20), S. 48; ausf. *Bechler*, Informationseingriffe durch intransparenten Umgang mit personenbezogenen Daten, 2010, S. 41 ff.

[43] Am Beispiel des Rechts auf „Vergessenwerden" *Spiecker gen. Döhmann*, KritV 2014, 28. Zum Vollzugsproblem auch *Schoch*, in: FS Stern, 2012, S. 1491 (1499, 1508), wonach die Überforderung des Gesetzgebers am Ende zur faktischen Unwirksamkeit des geschaffenen Rechts führen könne.

[44] Vgl. *Bull* (Fn. 20), S. 36 ff., der sich pauschal gegen die Ableitung von Prinzipien des Datenschutzrechts aus der Verfassung wendet.

[45] Im Urteil zur automatischen Kennzeichenerfassung hat das BVerfG bekräftigt, dass der grundrechtliche Schutz nicht schon deshalb entfällt, weil die betroffene „Information" öffentlich zugänglich ist, vgl. BVerfGE 120, 378 (399).

[46] Statt vieler *Schoch* (Fn. 43), S. 1507 f.

[47] *Schoch* (Fn. 43), S. 1509.

[48] *Schoch* (Fn. 43), S. 1509, 1512. Ähnlich *Bull* (Fn. 20), S. 40 ff., 57 ff., 94 ff. Zu weit *Nettesheim* (VVDStRL 70 [2011], 7 [43]), der auf einen Privatsphärenschutz in öffentlichen Räumen ganz verzichten will.

[49] EuGH, Urt. v. 13.5.2014 – C-131/12 (Google Spain), Rn. 80 ff.

[50] *Trute* (Fn. 3), Kap. 2 Rn. 10 f.

dungskontexte zugunsten eines ex post Rechtsschutzes verzichtet würde.[51]

Reduziert man das Recht auf informationelle Selbstbestimmung auf einen Missbrauchsschutz, wäre die Reichweite des Datenschutzrechts begrenzt. Die maßgeblichen Vorgaben für die Informationsordnung müssten anderswo gesucht werden. Das wäre deutlich mehr als eine bloße Nachjustierung, sondern würde die bereits vorhandenen Strukturierungspotentiale des Rechts auf informationelle Selbstbestimmung für die Ausgestaltung des Datenschutzes als Bestandteil der Informationsordnung verspielen.

b) Datenschutz als instrumentelle Freiheit?

Ähnlich argumentiert die Kritik an der Grundkonzeption, soweit das Recht auf informationelle Selbstbestimmung als Gewährleistung „um ihrer selbst willen" verstanden wird. *Gabriele Britz* stellt im Anschluss an *Marion Albers* heraus, dass es eine eigentumsanaloge Informationsverfügungsbefugnis nicht geben könne, weil Informationen ein antizipiertes oder real vollzogenes soziales Phänomen fremder Sinnkonstruktion über personenbezogene Daten sind. Subjektive Beobachtungen und Sinnkonstruktionen anderer ließen sich schlicht nicht beherrschen. Demgegenüber wäre ein Beherrschungsrecht an personenbezogenen Daten zwar „interaktionsfrei" zu denken. Beeinträchtigungen resultieren aber erst aus der Beobachtung und subjektiven Interpretation dieser Daten durch andere und deren daran anschließende Erwartungen und Maßnahmen bzw. aus der Antizipation von Beobachtung und nachteiliger Folge. Gefährdungen und Beeinträchtigungen entstehen eben erst in den Verwendungskontexten, in denen Informationen über Betroffene generiert werden.[52] Erst auf diese Verwendungszusammenhänge könne sich der Grundrechtsschutz im Kern beziehen, nicht auf die Preisgabe von Daten an sich.

Daraus wird nun aber gefolgert, das Recht auf informationelle Selbstbestimmung sei nur ein instrumentelles Recht im Dienste anderer Freiheitsgewährleistungen.[53] An die Stelle einer eigentumsanalog konzipierten ursprünglichen Verfügungsbefugnis tritt eine Konzeption, die im Recht auf informationelle Selbstbestimmung eine dienende Freiheit versteht, die zur Sicherung anderer Verhaltensfreiheiten zum Einsatz kommt. Das kulminiert in der Feststellung, die Abstützung auf den Gedanken der Selbstbestimmung sei missverständlich: Die Einräumung einer Datenverfügungsbefugnis als rechtliches Instrument zur Regulierung der Entstehung und Verwendung von Informationen könne mittelbar materielle Selbstbestimmung fördern. Aber eine eigenständige Komponente des Selbstbestimmungsgedankens werde die Datenverfügungsbefugnis nicht. Die informationelle Selbstbestimmung sei lediglich ein Mittel der Sicherung von Verhaltensfreiheit, die ihrerseits im Selbstbestimmungsgedanken wurzelt. Dafür greife die Verankerung allein im allgemeinen Persönlichkeitsrecht zu kurz, weil sich die Notwendigkeit des Schutzes häufig auf Aspekte äußerer Entfaltungsfreiheit stütze, die durch die speziellen Freiheitsrechte und subsidiär die allgemeine Handlungsfreiheit, nicht aber das verfassungsrechtliche Persönlichkeitsrecht geschützt werden.[54]

Die soziale Dimension von Informationen hat das BVerfG bereits im Volkszählungsurteil anerkannt, aber grundrechtsdogmatisch als ein Problem kollidierender Rechte in der Schrankendogmatik verarbeitet. Gerade das impliziert die Annahme eines Rechts, das missverständlich als Verfügungsbefugnis über die „eigenen" Daten verstanden wird. Wichtig wird in dieser Neukonzeption die Unterscheidung zwischen Selbstbestimmung als materielles Recht und instrumentelles Recht. Das Recht auf informationelle Selbstbestimmung sei nur letzteres, verstanden als Sicherung von Verhaltensfreiheit. Es sei konzeptionell auf den Schutz anderer, eben der gefährdeten Freiheiten ausgerichtet und deshalb ein *akzessorisches* Recht. Wegen der Ausrichtung auf den Schutz anderer Freiheiten werde nicht jede Informationsmaßnahme vom Grundrecht auf informationelle Selbstbestimmung erfasst, sondern nur solche, die eine Freiheit konkret beeinträchtigen oder die besondere Gefahr einer Freiheitsbeeinträchtigung begründen.

Ist aber noch nicht erkennbar, welches Rechtsgut nachteilig betroffen ist, vermag ein bloß akzessorischer Schutz nicht zu überzeugen. Für abstrakte Gefährdungslagen bleibt ein selbstständiger Schutz über Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG unverzichtbar, mag dieser auch weniger abwehrrechtlich als objektivrechtlich zu begründen sein, worüber sich ein differenziertes Schutzkonzept mit subjektivrechtlichen Einschlägen entwickeln ließe. Versteht man das Recht auf informationelle Selbstbestimmung demgegenüber allein instrumentell, wäre das Datenschutzrecht als solches kaum in der Lage, wesentliche Beiträge zur Ausgestaltung der Informationsordnung zu leisten. Wir könnten den Datenschutz getrost den Experten überlassen.

c) „Zweiebenenkonzeption" für den Daten- und Informationsumgang

Statt die Strukturierungsvorgaben allein unter Verhältnismäßigkeitsgesichtspunkten zu entwickeln, setzt die „Zweiebenenkonzeption" auf objektivrechtliche Pflichten, die nicht bloß punktuell bei Eingriffen in den nebulösen Schutzbereich des informationellen Selbstbestimmungsrechts subjektiv angestoßen werden, sondern eine vorgelagerte Strukturierungsfunktion haben, die für bestimmte Fragen subjektivrechtlich aufgeladen sein kann.[55]

Diese Konzeption sieht in den speziellen Freiheitsgewährleistungen des Grundgesetzes wichtige Anküpfungspunkte für den Datenschutz. Allerdings verdeutlichen gerade die Nachbarwissenschaften die Selektivität des traditionellen Freiheitsschutzes, der die soziale Konstitution der Freiheit weitgehend ausblendet. Erforderlich ist ein um die Sozialität

[51] Dagegen auch *Spindler*, Persönlichkeitsschutz im Internet: Anforderungen und Grenzen einer Regulierung, Gutachten F zum 69. Deutschen Juristentag, 2012, F 101 f.

[52] *Britz* (Fn. 6), S. 567.

[53] Vgl. *Britz* (Fn. 6), S. 566 ff.; *Poscher*, in: Gander (Hrsg.), Resilienz in der offenen Gesellschaft, 2012, S. 167 (178 ff.).

[54] *Britz* (Fn. 6), S. 573.

[55] Grundlegend *Albers*, Informationelle Selbstbestimmung, 2005, passim.

des Individiuums erweiteres Grundrechtsverständnis, das den Schutz im Hinblick auf den Umgang anderer mit personenbezogenen Informationen einschließen muss. Das gilt auch für die Aktivierung von Art. 2 Abs. 1 GG zum Schutz personeller Identität, Individualität oder sozialer Positionen.

Die Pointe liegt freilich in der Erweiterung der abwehrrechtlichen Perspektive. Abwehrrechtliche Gehalte sind im Hinblick auf den Umfang mit personenbezogenen Daten bei den Schutzbereichen der Freiheitsrechte anzudocken, doch auf der vorgelagerten Ebene bestehe eine aus dem Recht auf informationelle Selbstbestimmung folgende objektivrechtliche Pflicht des Gesetzgebers zur Schaffung eines kommunikative Selbstbestimmung sichernden Informationsumgangs.[56] Wie auch anderswo schließen objektiven Strukturierungspflichten das Entstehen subjektiver Rechtspositionen nicht aus. So macht es Sinn, die phasenübergreifenden Maßgaben der Zweckfestlegung und der Zweckbindung ebenso wie das Regelungselement der Erforderlichkeit weniger aus dem Übermaßverbot als Konsequenz individueller Entscheidungsrechte hinsichtlich persönlicher Daten zu entwickeln, sondern aus objektivrechtlichen Verpflichtungen des Gesetzgebers. Aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG folgt auf einer grundlegend vorgelagerten Ebene die Verpflichtung zu einer sachgerechten und transparenzsichernden Gestaltung des Umgangs mit personenbezogenen Informationen und Daten, aber mit Blick auf die „Wissenskomponente" freier Entfaltung der Persönlichkeit auch zur Gewährleistung individueller Kenntnismöglichkeiten und Einflusschancen als Leistungsrechte.[57] Hinzu kommen Anforderungen an die Institutionalisierung adäquater Kontrollen, deren unionsrechtlich geforderte „Unabhängigkeit" mit sachlichen Anforderungen an eine wirksame Datenschutzkontrolle gerechtfertigt werden kann.[58]

Demnach ist keine „Instrumentalität" zugunsten anderer Freiheiten gefragt. Vielmehr sind passende „Abstimmungen" mit anderen informationsbezogenen Verfassungsvorgaben erforderlich, um zu einer angemessenen verfassungsrechtlichen Determination der einfachrechtlichen Ebene zu gelangen. Soweit am grundrechtlichen Topos „informationeller Selbstbestimmung" festgehalten wird, kann dafür weder allein der Gedanke der Persönlichkeitsentfaltung in der Privatsphäre noch ein übergreifender Aspekt der „Selbstbestimmung" die Funktion eines Leitbildes übernehmen. Gefährdungen des informationellen Selbstbestimmungsrechts ist durch aus seinen objektivrechtlichen Schichten entwickelten Anforderungen zu begegnen, die sich auf die Verwendungszusammenhänge beziehen, worüber Vorgaben an die Gesetzgebung für die Gestaltung von Informationszusammenhängen formuliert werden können, die dem Einzelnen durch Transparenz, Nachvollziehbarkeit und Beschränkung auf das Erforderliche die nötigen Selbstdarstellungsmöglichkeiten sichert.[59]

Mit dieser Konzeption des Rechts auf informationelle Selbstbestimmung wäre es möglich, das überkommene Datenschutzrecht informationsregulatorisch, aber nach Gefährdungslagen und Sachbereichen differenziert, fortzuentwickeln. Weder ein enges (oben a) noch ein instrumentelles (oben b), sondern nur ein den Umgang mit Informationen regulierendes Datenschutzrecht dürfte im Lichte des Rechts auf informationelle Selbstbestimmung und der Judikatur des BVerfG eine angemessene Folie für seine Neukonzeption sein.[60] Das aber verlangt, die informationelle Selbstbestimmung im Vorfeld von Gefährdungen spezieller Freiheitsrechte in den objektivrechtlichen Schichten als Vorgabe an den Gesetzgeber zu spezifizieren. Erforderlich ist ein „mehrdimensionales Konzept, das sein Gravitationszentrum in der kommunikativen Selbstbestimmung der Persönlichkeit hat und deren Leitbild nicht das Datengeheimnis, sondern die Wahrung von Selbstbestimmung in einer Datenverkehrsordnung" ist.[61] Gerade für die neue Welt des Datenschutzes mit den Herausforderungen durch Big Data kommt es darauf an, von der Fokussierung auf Begrenzungen der Datenerhebung und -verwertung Abstand zu nehmen und stärker die Ordnungsfunktionen des Rechts unter der Ermöglichungsfunktion technischer und selbstregulativer Schutzmechanismen herauszustellen. Der Verzicht auf informationelle Selbstbestimmung bzw. dessen Aufgehen im Persönlichkeitsrecht zugunsten einer Vorfeldsicherung spezieller Verhaltensfreiheiten würde den Datenschutz demgegenüber um eine wichtige Grundlage der Freiheitssicherung berauben.

Stattdessen müsste ein anspruchsvolles Konzept von Datenschutz, das wichtige Impulse für die Ausgestaltung der Rechtsordnung als Informationsordnung liefern könnte, ein auf die jeweiligen Gefährdungslagen reagierendes, aber vielschichtiges Bündel von Maßgaben und Rechten im Hinblick auf den Umgang mit personenbezogenen Informationen und Daten entwickeln.[62] Das Recht auf informationelle Selbstbestimmung bildet hierfür einen wichtigen Ausschnitt, worüber sich die Regelungen des einfachen Rechts problemgerecht gestalten und angemessen koordinieren ließen. Auf diese Weise könnten die Bausteine des Datenschutzrechts konsistenter an grundrechtliche Vorgaben und das weder aufzugebende noch zu überschätzende Recht auf informationelle Selbstbestimmung angeknüpft werden.

V. Internationale und europäische Herausforderungen

Die geschilderten Neukonzeptionen sind vor die internationalen und europäischen Herausforderungen des Datenschutzes gestellt. Angesprochen seien nur der NSA-Datenskandal, die

[56] Abl. *Nettesheim*, VVDStRL 70 (2011), 7 (29).
[57] *Albers* (Fn. 8), § 22 Rn. 78 ff.
[58] Vgl. *Roßnagel*, ZD 2015, 106.
[59] *Trute* (Fn. 3), Kap. 2 Rn. 32. Frühzeitig bereits *ders*., JZ 1998, 822 (825 f.). Dass Formen der Kontextsteuerung eine „signifikante Schutzbereichsverkürzung" oder in anderer Weise eine „Entleerung" des allgemeinen Persönlichkeitsrechts bewirken, lässt sich entgegen *Schoch* (Fn. 43), S. 1499 f. nicht darlegen. Es geht nicht darum, den Freiheitsschutz zu schmälern, sondern zu stärken.
[60] *Albers*, Rechtstheorie 33 (2002), 61 (81 f.); zust. *Cornils*, in: Hain u.a. (Hrsg.), Datenschutz im digitalen Zeitalter, 2015, S. 11 (37 f., 55 f.).
[61] *Trute* (Fn. 3), Kap. 2 Rn. 6.
[62] *Albers* (Fn. 55), S. 357 ff.; *dies*. (Fn. 8), § 22 Rn. 69 ff.

Sorge einer Verdrängung mitgliedstaatlicher Grundrechte durch die europäische Datenschutzgrundverordnung und das Phänomen von Big Data.

1. NSA und die Folgen

Die durch Edward Snowden angestoßenen Enthüllungen über die globale Überwachungspraxis der Geheimdienste werfen Fragen auf, für die es keine einheitliche Antwort gibt. Dass sich das Recht auf informationelle Selbstbestimmung in Deutschland nur begrenzt eignet, die heimliche Tätigkeit der US-amerikanischen National Security Agency (NSA) rechtsstaatlich zu disziplinieren, versteht sich von selbst. Aber auch das Völkerrecht stößt an Grenzen. Die völkerrechtlichen Regeln zum Datenschutz gewähren keine individuellen Rechte gegen Überwachungsmaßnahmen von Nachrichtendiensten.[63] Das wirft die Frage nach der Rolle des europäischen Unionsrechts auf.[64]

Es liegt auf der Hand, dass die Schutzmechanismen des Unionsrechts gegenüber den Mitgliedstaaten der Europäischen Union leichter durchsetzbar sind als gegenüber den USA. Mit Blick auf das TEMPORA-Programm des britischen Geheimdienstes GCHQ kommt ein Vertragsverletzungsverfahren nach Art. 258 AEUV gegen Großbritannien mit der Begründung in Betracht, dass die umfassende und anlasslose Überwachung überwiegend ausländischer Kommunikationsteilnehmer gegen das Datenschutzgrundrecht (Art. 8 GRCh) und das Diskriminierungsverbot aus Gründen der Staatsangehörigkeit (Art. 18 AEUV) verstößt.[65]

Aber auch Legalitätsbekundungen der amerikanischen Behörden mit Blick auf die Aktivitäten der NSA[66] sind unionsrechtlich nicht einfach hinzunehmen. So ist nach Art. 25 Abs. 1 der Datenschutz-Richtlinie die Übermittlung personenbezogener Daten in einen Drittstaat nur zulässig, wenn dieser ein angemessenes Schutzniveau gewährleistet. In der Safe-Harbor-Absprache haben sich die USA verpflichtet, die europäischen Datenschutzstandards einzuhalten, was die Europäische Kommission veranlasste, durch die Entscheidung 2000/250/EG festzustellen, dass aus EU-Sicht ausreichende Datenschutzstandards in den USA bestehen. Diese Entscheidung, die eine zentrale Grundlage für ökonomische Transaktionen amerikanischer Unternehmen in der EU bildet, kann von der Kommission überprüft und gegebenenfalls aufgehoben werden.[67] Zudem verleiht Art. 3 Abs. 1 dieser Entscheidung den Datenschutzbehörden der Mitgliedstaaten die Befugnis, zum Schutz von Privatpersonen bei der Verarbeitung personenbezogener Daten die Datenübermittlung an eine Organisation auszusetzen, wenn eine hohe Wahrscheinlichkeit besteht, dass die Grundsätze des Datenschutzes verletzt werden. Verwiesen wird auf die Befugnisse der nationalen Datenschutzbehörde und damit auf § 38 Abs. 5 BDSG, wonach die Landesdatenschutzbehörde zur Gewährleistung der Einhaltung der datenschutzrechtlichen Bestimmungen Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten anordnen kann. Das bedeutet, dass ungeachtet aller faktischen Schwierigkeiten schon de lege lata einem Unternehmen, das amerikanische Cloud-Dienste wie Dropbox oder iCloud einsetzt, die Übermittlung von Personaldaten in diese Dienste untersagt werden kann.[68]

Man kann sich fragen, ob der NSA-Skandal als Symbol der Internationalisierung der Herausforderungen des Datenschutzes zu einer Renaissance der grundrechtlichen Schutzpflichten führen wird.[69] Das betrifft weniger die verfassungsrechtliche Ebene, wo die Figur grundsätzlich anerkannt, wenn auch nur schwer gegenüber dem Gesetzgeber operationalisierbar ist.[70] Effektiveren Schutz könnte die Aktivierung unionsrechtlicher Schutzpflichten bieten. Zwar ist die Rechtsprechung bislang durch Zurückhaltung in der Annahme grundrechtlicher Schutzpflichten gekennzeichnet. Weil das europäische Datenschutzrecht jedoch durch einen grundsätzlichen Gleichklang der Anforderungen gegenüber staatlichen und privaten Akteuren geprägt ist, das Handeln privater Akteure aber diesseits einer Zurechnung zum Staat nicht als Eingriff gewertet werden kann, könnte sich gerade der Daten-

---

[63] Näher *Aust*, AVR 52 (2014), 375.

[64] Näher *Ewer/Thienel*, NJW 2014, 30.

[65] Vgl. *Schmahl*, JZ 2014, 220 (226); *Mayer*, Mit Europarecht gegen die amerikanischen und britischen Abhöraktionen?, Teil 2: GCHQ, VerfBlog 2013/11/18, abrufbar unter http://www.verfassungsblog.de/mit-europarecht-gegen-amerikanischen-und-britischen-abhoeraktionen-teil-2-gchq (22.5.2015). Soweit ein Grundrecht vor dem Inkrafttreten der Charta oder als Ausprägung sekundärrechtlicher Vorschriften anerkannt war, kommt es auf das im Protokoll Nr. 30 erklärte Opt Out des Vereinigten Königreichs nicht an, vgl. EuGH, Urt. v. 21.12.2011 –C-411/10 und C-493/10 (N.S./Secretary of State for the Home Department) = Slg 2011, I-13991, Rn. 122.

[66] Zur Diskussion in den USA *Gärditz/Stuckenberg*, JZ 2014, 209.

[67] So die Art. 29-Arbeitsgruppe nach Art. 29 Datenschutz-Richtlinie in einem Brief v. 13.8.2013, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130813_letter_to_vp_reding_final_en.pdf. (22.5.2015). Siehe auch *Dix*, Safe Harbor am Ende? Eine Betrachtung aus aufsichtsbehördlicher Sicht, Vortrag beim 9. Europäischen Datenschutztag am 28.1.2015 in Berlin, ebenfalls im Internet abrufbar unter http://www.datenschutz-berlin.de/attachments/1089/741_943_1.pdf? (22.5.2015)

[68] So die gemeinsame Erklärung der Datenschutzbeauftragten des Bundes und der Länder vom Juli 2013, vgl. Pressemitteilung v. 24.7.2013, abrufbar unter http://www.datenschutz-bremen.de/sixcms/detail.php?gsid=bremen236.c.9283.de (22.5.2015). Zum Ganzen *Mayer*, Mit Europarecht gegen die amerikanischen und britischen Abhöraktionen?, Teil 1: NSA, VerfBlog 2013/11/18, im Internet abrufbar unter http://www.verfassungsblog.de/mit-europarecht-gegen-amerikanischen-und-britischen-abhoeraktionen-teil-1-nsa. (22.5.2015)

[69] Zu den Grenzen *Lenski*, ZG 2014, 324.

[70] Zu den Schutzpflichten des Staates im vorliegenden Kontext *Hoffmann-Riem*, JZ 2014, 53 (56 f.); *Deiseroth*, DVBl 2015, 197 (199 ff.); *Hahn/Johannes/Lange*, DuD 2015, 71.

schutz für eine Aktivierung datenschutzrechtlicher Schutzpflichten anbieten. Ein Beispiel liefert der Facebook-Datentransfer in die USA bzw. die NSA für das PRISM-Überwachungsprogramm. Hier wird mit Spannung das Urteil des EuGH in der Rechtssache Schrems erwartet.[71]

2. Europäische Datenschutzgrundverordnung: Verdrängung des Rechts auf informationelle Selbstbestimmung?

Ferner muss gesehen werden, dass das geltende Datenschutzrecht veraltet ist. Das gilt auch für die europäische Datenschutz-Richtlinie, die aus einer Zeit stammt, in der die heutigen technischen und wirtschaftlichen Möglichkeiten der Datenspeicherung und -verwertung noch nicht bekannt waren. Soll die Weiterentwicklung des Datenschutzes nicht der Rechtsfortbildung des EuGH überlassen bleiben, wäre ein zügiger Abschluss der Verhandlungen zu der seit Jahren diskutierten, aber namentlich von Deutschland blockierten Datenschutzgrundverordnung wünschenswert.

Gewiss stellt sich aus deutscher Sicht eine Reihe an Fragen. So ist der Bundesrat mit einer Subsidiaritätsrüge nach Art. 12 EUV i.V.m. Protokoll Nr. 2 über die Anwendung der Grundsätze der Subsidiarität und Verhältnismäßigkeit der Wahl des Instruments einer Verordnung nach Art. 288 Abs. 2 AEUV mit dem Versuch einer Vollregelung des Datenschutzes für den öffentlichen und nicht-öffentlichen Bereich entgegen getreten.[72] Die bereichsspezifischen Regelungen für den Umgang mit personenbezogenen Daten würden unterlaufen und durch die Datenschutzgrundverordnung hinfällig. Mit der Zentralisierung der Datenschutzrechtsetzung entfielen nationale Umsetzungsspielräume, in denen die nationalen Grundrechte gelten. Vielfach wird die Sorge formuliert, damit wären Ausgestaltungsvorgaben nicht mehr dem Recht auf informationelle Selbstbestimmung, sondern nur noch dem substanziell für schwächer gehaltenen Datenschutzgrundrecht aus Art. 8 GRCh zu entnehmen.[73]

Aber es muss gesehen werden, dass die Kritik in weiten Teilen aufgegriffen wurde und eine Reihe von Öffnungen für nationale Regelungen vorgesehen ist. Zwar bleibt es bei den abstrakten Erlaubnistatbeständen des Art. 6 des Verordnungsvorschlags. Aber Art. 6 Abs. 3 lit. b in der Fassung der Entschließung des Europäischen Parlaments[74] erlaubt den Mitgliedstaaten die Einzelheiten der Erlaubnistatbestände selbst zu regeln. Zudem reduzierte das Parlament die Fülle an Befugnissen der Kommission zur delegierten Rechtssetzung nach Art. 290 AEUV und für Durchführungsrechtsakte nach Art. 291 Abs. 2 AEUV. Stattdessen ist ausdrücklich ein Umsetzungsspielraum der Mitgliedstaaten vorgesehen, was mancher Kritik die Grundlage nimmt.[75] Auch die Betroffenenrechte sind präziser geregelt. Dazu gehört die semantische Abrüstung im Hinblick auf das in Art. 17 des ursprünglichen Verordnungsentwurfs vorgesehene Recht einer Person, vergessen zu werden, das in seiner starken Fassung mit einer Verpflichtung des Verarbeiters, dafür zu sorgen, dass die verbreitete Information auch bei denen gelöscht wird, an die Daten übermittelt wurden, kaum praktikabel gewesen wäre.[76]

Es ist auch nicht so, dass mit einem Inkrafttreten der Datenschutzgrundverordnung die Rechtsprechung des BVerfG zum informationellen Selbstbestimmungsrecht obsolet wird. Dass mit der Neuregelung des Datenschutzes auf Unionsebene der nationale Grundrechtsschutz verloren gehe, lässt sich so pauschal nicht sagen. Soweit die Datenschutzgrundverordnung den Mitgliedstaaten explizit Spielräume belässt, werden die Unionsgrundrechte nicht verdrängt, aber die Anwendung nationaler Grundrechte auch nicht versperrt.[77] Zwar bleiben Unsicherheiten, die nicht zuletzt dadurch befördert wurden, dass sich das BVerfG veranlasst sah, die Anwendung der Unionsgrundrechte im Fall der Antiterrordatei ohne Not auszuschließen.[78] Wer aber mit der Verteidigung europäischer Datenschutzstandards in der Welt mit guten Gründen auf das Unionsrecht setzt, erhält – gewissermaßen als Schatten[79] – die Unionsgrundrechte, die in der Hand des EuGH keine Bedrohung für die Grundrechtskulturen der Mitgliedstaaten darstellen und das Recht auf informationelle Selbstbestimmung auch nicht verkürzen müssen.

---

[71] Az. C-362/14. Es handelt sich um ein Vorabentscheidungsersuchen des Irischen High Court, demzufolge es Beweise gebe, dass Facebook der NSA den massenhaften und undifferenzierten Zugriff auf persönliche Daten ermögliche. Insoweit stellt sich die Frage, ob die Europäische Kommission den grundrechtlichen Schutzpflichten aus Art. 8 GRCh durch eine Aufhebung der Entscheidung 2000/250/EG zur Safe-Harbor-Absprache mit den USA entsprechen *muss*.

[72] BR-Drs. 52/12, S. 1.

[73] Statt vieler *Masing*, SZ v. 9.1.2011, S. 10, abrufbar unter: http://www.datenschutzbeauftragter-online.de/wp-content/uploads/2012/01/20120109_SZ_Masing_Datenschutz.pdf (22.5.2015); *Roßnagel*, DuD 2012, 553 f.; *Roßnagel/Kroschwald*, ZD 2014, 495.

[74] Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr = P7_TA-PROV(2014)0212.

[75] Vgl. *Albrecht*, in: Hain u.a. (Hrsg.), Datenschutz im digitalen Zeitalter, 2015, S. 133 ff.; anders, aber wenig überzeugend *Pötters*, RDV 2015, 10.

[76] Vgl. *Hornung/Hofmann*, JZ 2013, 163.

[77] Vgl. *Franzius*, EuGRZ 2015, 139 (141 ff.); skeptischer *Cornils* (Fn. 60), S. 14 ff.

[78] BVerfGE 133, 277 (316); dazu *Volkmann*, Jura 2014, 820. Umgekehrt lässt der EuGH bislang wenig Bereitschaft erkennen, den Mitgliedstaaten die Ausfüllung sekundärrechtlicher Spielräume nach nationalen Grundrechten zu überlassen, vgl. EuGH, Urt. v. 24.11.2011 – C-468/10 und C-469/10 (ASNEF), Rn. 40, 43.

[79] *Lenaerts*, AnwBl 2014, 772 mit dem zweifelhaften Bild, so wie ein Gegenstand die Konturen seines Schattens forme, bestimme auch das Unionsrecht die Konturen der Charta. Danach formen nicht die Grundrechte das System, sondern das System die Reichweite der Grundrechte, krit. *Callewaert*, ZEuS 2014, 79 (89 f.).

3. Informationelle Selbstbestimmung im Zeichen von Big Data

Weder die Reaktionen auf die NSA-Affäre noch die EU-Datenschutzgrundverordnung liefern zufriedenstellende Antworten auf die zentralen Herausforderungen durch Big Data, die sich durch drei Dimensionen charakterisieren lässt: Erstens verweist Big Data auf das quantitative Anwachsen von Datensätzen auf der globalen Ebene. Die Informationsgesellschaft produziert immer mehr Daten, die immer leichter und kostengünstiger gespeichert werden können. Zweitens – und hier liegt der Kern von Big Data – wird mit der technischen, wirtschaftlichen und sozialen Möglichkeit gerechnet, immer detailliertere Informationen aus diesen Datensätzen und ihrer Verknüpfbarkeit herauslesen zu können, nicht zuletzt um auf dieser Grundlage Persönlichkeitsprofile zu entwickeln und auf das Verhalten der Menschen Einfluss zu nehmen. Damit verbunden erodieren drittens überkommene Vorstellungen von Kausalität. Es geht Big Data nicht einfach um die Maximierung von Wissen, sondern um Wahrscheinlichkeiten, die sich mit Hilfe von neuen Algorithmen berechnen lassen. Soll darüber die Zukunft vorhersehbar werden, brauche es eine weitreichende Erfassung von Daten, die sich durch Zweckbindungen nur schwer rechtsstaatlich disziplinieren lassen.

Insoweit bricht Big Data mit einem zentralen, gerade aus dem Recht auf informationelle Selbstbestimmung entwickelten Prinzip des Datenschutzrechts, weil Daten ohne Zweck gesammelt und miteinander verknüpft werden. Das gebietet weniger die Verlängerung des „Abwehrdenkens" in die wirtschaftlich lukrative Welt von Big Data, sondern vielmehr die Suche nach neuen Trennungs- und Verknüpfungsregeln, die sich nur aus den objektiven Schichten informationeller Selbstbestimmung entwickeln lassen dürften. Jedenfalls werden moderne Regulierungskonzepte des Internets sich kaum allein in den tradierten, aber nicht auf die Online-Welt von Big Data – mit den wirtschaftlichen Konzepten des Profiling und Scoring[80] – zugeschnittenen Bausteinen eines urheberrechtsähnlichen Rechts auf informationelle Selbstbestimmung ausbuchstabieren lassen.

Datenschutz, so formuliert es *Johannes Masing*, schützt schon dann, wenn es noch nicht wehtut.[81] Das sei die Pointe des Datenschutzes, denn „wenn wir warten, bis sich die gespeicherten Daten unmittelbar in Maßnahmen niederschlagen, brauchen wir eigentlich keinen Datenschutz, sondern nur Schutz gegen die Maßnahmen". Freilich symbolisiert Big Data das Paradox, dass Bürger trotz der Datenakkumulation, die über Präferenzen und damit auch Eigenschaften der Nutzer vermehrt Auskunft gibt, personenbezogene Daten mehr oder weniger freiwillig preisgeben.[82] Insoweit hat, worauf *Hans-Heinrich Trute* hingewiesen hat, der Zuwachs an Informationsvorgängen mit personenbezogenen Daten im weltweiten Maßstab neue Gefährdungen durch weitreichende „Möglichkeiten der Dokumentation und Manipulation digitalisierter personenbezogener Informationen, ihrer Kommerzialisierung und eines eher inkrementalen Verlustes von Freiheit durch Gewöhnung, Anpassung und Konventionsbildung" zur Folge.[83] Hier eine Verantwortung hoheitlicher Stellen hervorzuheben, hat wenig mit Paternalismus zu tun, muss aber die veränderten gesellschaftlichen Einstellungen zur Kenntnis nehmen. Die Frontstellung liegt weniger in der Abwehr staatlicher Datenerhebung, sondern unter der Nivellierung der Entgegensetzung staatlicher oder privater Datenschutz- und Datennutzungsinteressen in der Nachfrage nach Informationsteilhabe des Bürgers an Informationsbeständen sowie im Neuzuschnitt der Schutzmechanismen vor privatem Datenhunger.

Erforderlich wird ein transnationales Datenschutzrecht, das stärker als bisher auf die Zunahme privater Gefährdungen der Selbstbestimmung zugeschnitten ist, aber auch die unions- und völkerrechtlichen Schutzmechanismen in den Blick zu nehmen hat, ohne dadurch deren Aufnahme und Einbettung im nationalen Datenschutzrecht zu vernachlässigen.[84] Insoweit hat die Ausdifferenzierung der Regulierungskonzepte neben der Bedeutung privater Gefährdungspotentiale die Ebenenverschränkungen zu berücksichtigen, was zu der Frage führt, inwieweit den nationalen Zielen des Datenschutzes auf Unionsebene entsprochen werden kann. Hierfür sollte man sich von der Vorstellung einer pauschalen Übertragung des Rechts auf informationelle Selbstbestimmung auf die Unionsebene lösen.[85] Die never ending story um die Vorratsdatenspeicherung[86] zeigt, dass effektiver Schutz auch vom EuGH[87] zu erwarten ist, der in seinem Google-Urteil[88] trotz aller Kritik[89] seine Bereitschaft für innovative Lösungen

[80] Unergiebig BGH, Urt. v. 28.1.2014 – VI ZR 156/13 = NVwZ 2014, 747.

[81] *Masing*, VVDStRL 70 (2011), 86.

[82] Ob die in den Allgemeinen Geschäftsbedingungen von Facebook vorgesehene Einwilligung für die Weitergabe personenbezogener Daten ausreicht, kann bezweifelt werden. Hier müsste es darum gehen, die datenschutzrechtlichen Gehalte des europäischen Kartellrechts stärker in den Blick zu bekommen. Datenschutzrecht ist nicht nur Technikrecht, sondern auch Wettbewerbsrecht.

[83] *Trute* (Fn. 3), Kap. 2 Rn. 4.

[84] Allg. *Franzius*, Recht und Politik in der transnationalen Konstellation, 2014, S. 96 ff.

[85] Anders *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl. 2011, Art. 8 GRCh Rn. 1, der von der Existenz eines Rechts auf informationelle Selbstbestimmung auf Unionsebene ausgeht. Der EuGH nimmt Anleihen an der vom BVerfG entwickelten Figur, versteht informationelle Selbstbestimmung aber anders.

[86] Anders *Leutheusser-Schnarrenberger* (DuD 2014, 589) mit der Hoffnung auf ein Ende der Debatte. Davon kann heute, nachdem ein Vorschlag für eine deutsche Regelung einer anlasslosen, aber begrenzten Vorratsdatenspeicherung angekündigt ist, keine Rede mehr sein.

[87] Nachdrücklich *Bäcker*, Jura 2014, 1263.

[88] EuGH, Urt. v. 13.5.2014 – C-131/12 (Google Spain), Rn. 99.

[89] Befürchtet wird, dass die Balance zwischen Kommunikationsfreiheit und Persönlichkeitsschutz aus den Augen gerät, vgl. *Masing*, Vorläufige Einschätzung der Google-Entscheidung des EuGH, VerfBlog 2014/8/14, abrufbar unter

unter Beweis gestellt hat. Das Recht auf informationelle Selbstbestimmung wird dadurch nicht verdrängt, in seiner Bedeutung für die Anleitung des Gesetzesrechts aber relativiert. Ob es ratsam ist, auf einen Export dieser dogmatischen Figur zu setzen, erscheint zweifelhaft. Dass die informationelle Selbstbestimmung auf Unionsebene nicht schutzlos ist, wird kaum zu bestreiten sein, mag man auch gut beraten sein, sich nicht allein auf das Unionsrecht und den EuGH zu verlassen.

http://www.verfassungs-blog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh (22.5.2015). Positivere Einordnung: *Spiecker gen. Döhmann*, in: Hain u.a. (Hrsg.), Datenschutz im digitalen Zeitalter, 2015, S. 61 (78 ff.).