Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 469

Eingeschränkte Selbstbestimmung im Onlineverkehr: Stärkung der Einwilligungserklärung durch Einführung vorformulierter Datenschutzbestimmungen

Maren Pollmann[1], Dennis-Kenji Kipker[2]

Abstract: Die informationelle Selbstbestimmung wird im Online-Zeitalter zunehmend herausgefordert, indem eine immer weitergehende Verlagerung der Datenverarbeitung auf private Akteure stattfindet. Insbesondere die datenschutzrechtliche Einwilligung droht an Effektivität zu verlieren, da Datenschutzbestimmungen nicht nur hochkomplex ausgestaltet, sondern länger und umfassender denn je sind. Unter diesen Gesichtspunkten werden zunächst verschiedene aktuell diskutierte rechtliche Ansätze vorgestellt, die der Autonomie über die eigenen Daten Rechnung tragen sollen. Im Anschluss an eine Bewertung der unterschiedlichen Vorschläge folgt die Feststellung, dass keine dieser Maßnahmen für sich genommen ausreicht, um den Persönlichkeitsschutz im Internet zu gewährleisten. Vorgeschlagen wird deshalb ein System vorformulierter Datenschutzbestimmungen, welches über die bloße datenschutzrechtliche Klauselkontrolle in AGB hinausgeht.

Keywords: Einwilligung, informationelle Selbstbestimmung, AGB-Kontrolle, Datenschutzbestimmungen

1 Einführung und Problemaufriss

Die hohe Innovationsgeschwindigkeit im Onlinebereich sowie neue Möglichkeiten zur Auswertung von Datensätzen, die in Sekundenschnelle Verknüpfungen zwischen unterschiedlichen Informationen herstellen können, stellen das geltende Datenschutzrecht und damit auch das Recht auf informationelle Selbstbestimmung mehr denn je auf die Probe. Insbesondere Privatunternehmen sammeln und verarbeiten personenbezogene Daten aus jeglichen Lebensbereichen mithilfe einer Vielzahl von internetfähigen Alltagsgeräten. Zudem wird schon lange über Mängel im Vollzug des Datenschutzrechts geklagt.[3] Umso dringender ist es daher, den Datenschutz an die neuen Gegebenheiten anzupassen und ihn derart zu stärken, dass eine hinreichend effektive Wahrnehmung der informationellen Selbstbestimmung erreicht werden kann. Dieser Beitrag stellt einige der neuen Problemlagen heraus und präsentiert anschließend weitere

[1] Universität Bremen, Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universitätsallee GW1, 28359 Bremen, m.pollmann@uni-bremen.de.
[2] Universität Bremen, Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universitätsallee GW1, 28359 Bremen, kipker@uni-bremen.de.
[3] Siehe dazu Ritter/Schwichtenberg, VuR 2016, 95 (96); Spiecker gen. Döhmann, in: Leible/Kutschke, Der Schutz der Persönlichkeit, S. 33.

Vorschläge und Ideen zum Schutz der informationellen Selbstbestimmung, speziell bezogen auf die datenschutzrechtliche Einwilligung.

2 Herausforderungen der informationellen Selbstbestimmung im Online-Zeitalter

2.1 Verlagerung auf private Akteure

Das Grundrecht auf informationelle Selbstbestimmung blickt bereits auf eine über 30-jährige Geschichte zurück. Als ein Recht, dessen Existenz und Schutzgewährleistungen im Wesentlichen auf dem technologischen Fortschritt im Bereich der automatisierten Datenverarbeitung begründet sind, unterliegt es einem steten Wandel. Insbesondere die modernen Online-Technologien fordern die individuelle Verwirklichung informationeller Selbstbestimmung stetig heraus, da die Geschäftsmodelle zahlreicher im Internet agierender Unternehmen auf der wirtschaftlichen Nutzung personenbezogener Daten basieren, so beispielsweise im Bereich kontextgesteuerter Werbeanbieter. Die Gefährdungslage für personenbezogene Daten, die sich aus dem Handeln solcher nicht-staatlichen Akteure ergibt, ist nicht mit der Entstehungsgeschichte und ursprünglichen Schutzrichtung des Grundrechts auf informationelle Selbstbestimmung identisch. Während es 1983 für den Fall des Volkszählungsgesetzes noch allein um den Schutz vor einer die Persönlichkeit über die Maße beeinträchtigenden staatlichen Datenverarbeitung ging[4] und diese durch das klassische Subordinationsverhältnis geprägt war, bei dem die Freiheit und die Rechte des Bürgers den Bindungen und rechtfertigungsbedürftigen Befugnissen des Staates gegenüberstehen,[5] spielt sich das Verhältnis zwischen Bürger und Unternehmen vielmehr auf einer Ebene der Gleichordnung ab. Trotz dieser zunächst formalen Gleichheit kann sich ein in der Intensität vergleichbares Gefährdungspotenzial für die informationelle Selbstbestimmung ergeben, das auf der „manchmal bestehenden Asymmetrie der Kräfteverhältnisse“[6] beruht. Es besteht also ein Machtgefälle zwischen den beiden Akteuren, das zuvorderst nicht durch das Einräumen von Abwehrrechten, sondern im Wesentlichen nur durch die Erfüllung staatlicher Schutzpflichten ausgeglichen werden kann.[7] Obwohl der Schutz der informationellen Selbstbestimmung ein hochrangiges Gut darstellt, ist er aber nicht frei von Beschränkungen. Jeder Einzelne ist als Bestandteil der Gesellschaft im Regelfall in diese eingebunden – und das auch in Bezug auf die Verarbeitung seiner personenbezogenen Daten.[8] Dies ist ebenso zu berücksichtigen, wenn es um die Informationsnutzung durch Unternehmen geht, sodass

[4] Gesetz über eine Volkszählung, Berufszählung, Wohnungszählung und Arbeitsstättenzählung (Volkszählungsgesetz 1983) vom 25. März 1982 (BGBl. I S. 369) - VZG 1983, BVerfGE 65, 1.
[5] Grimm, JZ 2013, 585 (587).
[6] Grimm, JZ 2013, 585 (587).
[7] So auch Grimm, JZ 2013, 585 (587).
[8] Vgl. BVerfGE 65, 1 (40).

im Rahmen der hier stattfindenden Interessenabwägung nicht nur das Grundrecht auf informationelle Selbstbestimmung, sondern auch die Entscheidung zu wirtschaftlicher Aktivität und damit die Unternehmensfreiheit sowie die Allgemeine Handlungsfreiheit (Artt. 12 Abs. 1, 2 Abs. 1 GG) als gegenläufige Interessen einbezogen werden müssen und nicht von vornherein geringer als die informationelle Selbstbestimmung bewertet werden dürfen.[9] Soweit deshalb Lösungsansätze zum Schutz einer zukünftigen, zeitgemäßen informationellen Selbstbestimmung entwickelt werden, müssen sich diese auch an den technologisch möglichen und wirtschaftlich aufgegriffenen Nutzungsmöglichkeiten personenbezogener Daten orientieren.

2.2 Begrenzte Effektivität der datenschutzrechtlichen Einwilligung

Die Zulässigkeit einer Datenverarbeitung sowohl im öffentlichen als auch im nicht-öffentlichen Bereich wird durch das Verbotsprinzip mit seinen gesetzlichen Erlaubnistatbeständen bestimmt. Die Verarbeitung personenbezogener Daten ist danach grundsätzlich verboten. Lediglich eine individuelle Einwilligung des Betroffenen oder ein gesetzlicher Erlaubnistatbestand können dem Datenverarbeiter als Legitimationsgrundlage dienen.[10] Auf diese Weise setzt das Verbotsprinzip die bereits vom Bundesverfassungsgericht geforderte Entscheidungsfreiheit des Einzelnen, über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, um.[11]

Die Erteilung einer Einwilligung durch den von der Datenverarbeitung Betroffenen stellt als stärkster Ausdruck der informationellen Selbstbestimmung und der individuellen Entfaltungsfreiheit hierbei den zentralen Legitimationstatbestand dar. Dennoch unterliegt die Anwendung des Verbotsprinzips insbesondere im Verhältnis zwischen Privaten häufiger Kritik.[12] Infolge dieser wird zum Teil eine striktere Trennung der Regelungen der öffentlichen Datenverarbeitung durch den Staat als unmittelbaren Grundrechtsadressaten und der Datenverarbeitung zwischen Privaten, die nur mittelbar an die Grundrechte gebunden sind, gefordert.[13] Aufgrund der hohen Datennutzungserfordernisse vieler Dienstleistungsunternehmen ist das Institut der datenschutzrechtlichen Einwilligung für den Online-Verkehr aber auch gleichsam essenziell, denn sie ermöglicht für die verarbeitende Stelle eine flexible Alternative zu den engen gesetzlichen Ausnahmetatbeständen. Ihre Wirksamkeit hängt jedoch von der Einhaltung gesetzlicher Voraussetzungen ab. Insbesondere die notwendige Informiertheit der Einwilligung sowie das Erfordernis einer bewussten und eindeutigen Erklärungshandlung stellen dieses Instrument regelmäßig auf die Probe. Dies verdeutlicht unter anderem ein Blick auf das vielzitierte Beispiel der Datenschutzbestimmungen des sozialen Netzwerks Facebook: Durch die darin enthaltenen Verweise auf die Klauseln integrierter Dienste und Anwendungen steigt die

[9] Bull, NJW 2006, 1617 (1622).
[10] Scholz/Sokol, in: Simitis, BDSG, § 4, Rn. 2.
[11] BVerfGE 65, 1 (42).
[11] S. unter 3.3.
[13] Masing, NJW 2012, 2305 (2307).

Menge an Information für den Nutzer erheblich an.[14] Dies hat zur Folge, dass der Einzelne angesichts der Vielzahl an datenschutzrechtlich relevanten Vorgängen faktisch nicht in der Lage ist, sich umfassend über die Verarbeitung seiner personenbezogenen Daten zu informieren. Der ohnehin schon häufige Fall, dass ein Betroffener für die Leistung eines bestimmten Onlinedienstes im Gegenzug seine personenbezogenen Daten in einem für ihn nicht nachvollziehbaren Umfang preisgeben muss, ohne die Reichweite seiner Einwilligung absehen zu können, darf durch derlei Anbieter nicht zum Regelfall werden. Ein solches Ergebnis widerspräche nicht nur dem Grundgedanken der informationellen Selbstbestimmung, sondern würde das Instrument der Einwilligung letzten Endes ad absurdum führen.

Des Weiteren bewirkt Big Data und die damit verbundene unbegrenzte Vernetzung von personenbezogenen Informationen, dass eine einmal gegebene Einwilligung für eine Vielzahl zum Teil unüberschaubarer Verarbeitungsvorgänge als Legitimationsgrundlage herangezogen werden kann. Das Verbotsprinzip kann dieser Entwicklung teilweise entgegentreten und den Einzelnen zumindest vor einem totalen Kontrollverlust über die Verwendung seiner persönlichen Daten schützen. Ein Festhalten an diesem Grundprinzip ist daher mehr als geboten. Doch angesichts der Defizite, die vor allem der Prozess der Einwilligungserteilung in der Praxis mit sich bringt, bedarf es neuer Regelungsinstrumente, welche die veränderten Rahmenbedingungen berücksichtigen und somit die Einwilligung zu einem wirksamen Instrument des Betroffenen machen, das seine schwächere Position gegenüber dem Online-Dienstleister auszugleichen vermag.

3 Bisher diskutierter Erkenntnisstand zum Schutz der informationellen Selbstbestimmung

Um dem Recht auf informationelle Selbstbestimmung auch im Zeitalter des unbegrenzten globalen Datenverkehrs noch zu hinreichender Wirksamkeit zu verhelfen, werden bereits seit mehreren Jahren unterschiedliche rechtliche Lösungsansätze diskutiert, die für sich betrachtet jedoch selten zu vollends befriedigenden Ergebnissen gelangen.

3.1 Eigentumsähnliche Ausgestaltung

Einige Vorschläge zur Verbesserung der informationellen Selbstbestimmung zielen darauf ab, das Recht am eigenen Datum zu einem eigentumsähnlichen Recht umzufunktionieren. Hierdurch soll Immaterialgüterschutz gewährt[15] oder aber ein eigenes Datenwirtschaftsrecht[16] geschaffen werden. Auch wenn es zunächst sinnvoll

[14] Buchner, DuD 2015, 402 (404).
[15] Kilian, in: Garstka/Coy, Wovon - für wen - wozu, S. 195 (211).
[16] Reiners, ZD 2015, 51; Seidel, ZG 2014, 153 (158)

scheinen mag, das Recht an der Nutzung personenbezogener Daten vorrangig zu monetarisieren, so besteht das Risiko, dass durch eine solche Verwirtschaftlichung des Persönlichkeitsschutzes dem informationellen Selbstbestimmungsrecht seine ideelle Basis entzogen wird. Obgleich personenbezogene Daten als Grundlage für die Geschäftsmodelle einiger großer Internet-Unternehmen wie beispielsweise Google oder Facebook dienen und ihnen die Eigenschaft als Ware somit nicht vollständig aberkannt werden kann, ist dies nicht ihr einziges oder gar ausschlaggebendes Merkmal. Vor allem die ursprüngliche Herleitung des Rechts auf informationelle Selbstbestimmung aus dem Menschenwürdegrundsatz darf nicht völlig außer Acht gelassen werden. Eine Ablehnung der eigentumsähnlichen Ansätze schließt jedoch nicht die Möglichkeit aus, dem Betroffenen durch zukünftige Anpassungen seines Rechts auf informationelle Selbstbestimmung auch eine gewisse wirtschaftliche Teilhabe an dem Umgang mit den personenbezogenen Daten einzuräumen.

3.2 Ausgestaltung als objektiv-rechtliche Teilhabeordnung

Andere Ansätze sehen vor, das Recht auf informationelle Selbstbestimmung in Abkehr vom subjektiv-rechtlichen Gehalt als objektiv-rechtliche Informationsordnung auszugestalten. Der einem solchen Verständnis entsprechende Grundrechtsgehalt setzt sich aus objektiven Wertentscheidungen zusammen und tritt in der Dogmatik neben die subjektiv-rechtliche Abwehrfunktion der Grundrechte.[17] Gemäß der objektiv-rechtlichen Teilhabeordnung muss der Staat die Grundrechte in seinen Entscheidungen berücksichtigen, sodass unterschiedlich ausgeprägte Pflichten zur Ausgestaltung der Rechtsordnung hergeleitet werden können.[18] Ihn kann beispielsweise eine staatliche Schutzpflicht treffen, der zufolge er der informationellen Selbstbestimmung auch zwischen Privaten zur Geltung verhelfen muss.[19] Eine weitere Ausprägung stellt der Grundrechtsschutz durch Organisation und Verfahren dar, welcher bereits im Volkszählungsurteil durch das Bundesverfassungsgericht als flankierende Maßnahme gefordert wurde.[20] Auf ebendiese objektiv-rechtliche Funktion der informationellen Selbstbestimmung stützen sich eine Reihe unterschiedlicher Ansätze zur Modernisierung des Grundrechts. Es soll dabei als ein Teilhaberecht ausgestaltet werden, das sich auf die Funktion des Datenschutzrechts als Kommunikationsordnung konzentriert und so dem Einzelnen ein Recht auf kommunikative Selbstbestimmung zuspricht.[21] Gerade für den elektronischen Privatrechtsverkehr geben die Ansätze zur objektiv-rechtlichen Gestaltung des informationellen Selbstbestimmungsrechts wichtige Impulse: So kann die Stärkung der Teilhabe des Einzelnen an datenschutzrechtlich relevanten Vorgängen einen entscheidenden Beitrag leisten, um dem Machtungleichgewicht zwischen global

[17] Bechler, Informationseingriffe durch intransparenten Umgang mit personenbezogenen Daten, S. 76.
[18] Bechler, Informationseingriffe durch intransparenten Umgang mit personenbezogenen Daten, S. 77.
[19] Britz, in: Hoffmann-Riem, Offene Rechtswissenschaft, S. 561 (585 f.).
[20] BVerfGE 65, 1 (58 f.).
[21] Schoch, in: Sachs/Siekmann, Der grundrechtsgeprägte Verfassungsstaat, S. 1491 (1499); Simitis, in: Simitis, BDSG, § 1, Rn. 36 f.

agierenden Unternehmen und Individuen entgegenzutreten. Zudem sind die von Hoffmann-Riem herausgestellten Möglichkeiten für einen effektiven Selbstschutz durch die Nutzer von großer Bedeutung. Hierzu ist neben der Förderung von sozialen und technischen Kompetenzen auch die Aufklärung durch Verbraucherverbände vorgesehen.[22] Die steigende Komplexität informationstechnischer Systeme erhöht jedoch auch die Herausforderungen, die mit der Realisierung des individuellen Selbstschutzes verbunden sind. So wird es auch für den technisch sachverständigen Bürger zunehmend schwieriger, die Datenverarbeitungsvorgänge zu überblicken und sein Handeln auf die Maximierung des Persönlichkeitsschutzes hin auszurichten.[23] Aus diesem Grund ist das Abstellen auf den individuellen Selbstschutz zwar notwendig, kann jedoch nicht die subjektive Dimension des informationellen Selbstbestimmungsrechts entbehrlich machen. Die Vorschläge, allein auf den objektiv-rechtlichen Gehalt des Grundrechts abzustellen, haben eine einseitige Konzeptionierung des Selbstbestimmungsrechts zur Folge, welche die Grundrechtsdogmatik nicht in ausreichendem Maße berücksichtigt.

3.3 Abkehr vom Verbotsprinzip

Weiters wird zur Novellierung des Rechts auf informationelle Selbstbestimmung die Abkehr vom bisher maßgebenden Verbotsprinzip der Datenverarbeitung diskutiert. Hierin wird teilweise dennoch eine Einschränkung der ebenfalls grundrechtlich geschützten Kommunikationsfreiheit gesehen, deren verfassungskonforme Wahrnehmung nur bei einer weiten Auslegung seiner Ausnahmen noch möglich sei.[24] Ebenso bewirke die weite Auslegung der Personenbezogenheit von Daten, dass ein Großteil der Kommunikation im Internet unter das Datenschutzrecht falle, was ein Durchsetzungshemmnis für die informationelle Selbstbestimmung zur Folge hat.[25] Mit dem Verbotsprinzip sei zudem die staatliche Schutzpflicht nicht erfüllt, da sie neben dem Persönlichkeitsschutz auch die Sicherstellung der größtmöglichen Entfaltungsfreiheit des Einzelnen umfasse.[26] Aller Kritik am Verbotsprinzip zum Trotz hätte jedoch der Einzelne ohne eine solche Lösung kaum mehr Möglichkeiten zu wissen, wer wann welche Daten von ihm erhebt und auf welche Weise verarbeitet. Um einem zunehmenden Kontrollverlust über die Verwertung der eigenen Daten entgegenzutreten, kann das Verbotsprinzip deshalb auch in Zukunft nicht entfallen. Dass ein Festhalten an diesem Prinzip geboten ist, zeigt neben der ausdrücklichen Normierung in Art. 8 Abs. 2 GR-Charta auch der europäische Reformprozess zur Datenschutzgrundverordnung, bei dem das Verbotsprinzip weder in einem der Entwürfe noch im vorausgehenden parlamentarischen Diskurs ausdrücklich infrage gestellt wurde.[27]

---

[22] Hoffmann-Riem, AöR 1998, 513 (536 f.).
[23] Bäcker, Der Staat 2012, 91 (112).
[24] Schneider, AnwBl. 2011, 233 (234); Härting, NJW 2013, 2065 (2067).
[25] Härting, in: Leible/Kutschke, Der Schutz der Persönlichkeit, S. 55 (58); Schneider, AnwBl. 2011, 233 (233).
[26] Giesen, CR 2014, 550 (552).
[27] Vgl. dazu jeweils Art. 6 der Entwürfe zur Datenschutzgrundverordnung von der Europäischen Kommission vom 25. Januar 2012 (KOM(2012) 11 endg., des Europäischen Parlaments vom 12. März 2014 und des Rats

3.4 Verknüpfung von Datenschutz und Wettbewerbsrecht

Einen entscheidenden Schritt zur Stärkung der informationellen Selbstbestimmung könnte eine engere Verzahnung zwischen dem Datenschutz- und dem Wettbewerbsrecht darstellen. Hier gilt es, bestehende Regelungen des UWG ausdrücklich für das Datenschutzrecht zu öffnen. Ein Rückgriff auf das Wettbewerbsrecht kann zum Persönlichkeitsschutz im Rahmen der Datenverarbeitung beitragen, indem es den Betroffenen eine Marktteilnehmerposition einräumt und hierdurch der kaum zu vermeidenden Entwicklung hin zu einer Kommerzialisierung personenbezogener Daten Rechnung trägt. Das Wettbewerbsrecht knüpft somit an den zunehmenden Vermögensaspekt von Informationen über Einzelpersonen an. Eine Verbindung der beiden Rechtsgebiete ermöglicht zudem, dass sich neben den Betroffenen auch Mitbewerber gegen unlautere Verhaltensweisen anderer datenverarbeitender Marktteilnehmer zur Wehr zu setzen können. Diese Option bietet das geltende Datenschutzrecht nicht, da es sich in der individuellen und behördlichen Rechtsdurchsetzung erschöpft.[28]

3.5 Neuausrichtung einzelner Elemente des Datenschutzrechts

Neben Ansätzen, die eine fundamentale Umstrukturierung des Datenschutzrechts fordern, wird auch vorgeschlagen, mithilfe einzelner Anpassungen der bestehenden Grundsätze eine Stärkung der informationellen Selbstbestimmung zu erreichen. Insbesondere Big Data und die damit verbundene unbegrenzte Vernetzung von personenbezogenen Informationen stellen das Institut der datenschutzrechtlichen Einwilligung vor eine Herausforderung, da diese grundsätzlich zeitlich nicht begrenzt ist und somit für eine Vielzahl zum Teil unüberschaubarer Verarbeitungsvorgänge als Legitimationsgrundlage herangezogen werden kann. Daher wird teilweise gefordert, die Einwilligung zeitlich zu befristen.[29] Eine solche zeitliche Begrenzung der Einwilligung scheint jedoch wenig praktikabel, da es nur schwer möglich ist zu kontrollieren, ob das jeweilige Unternehmen nach Ablauf der Zeit eine neue Einwilligung von dem Betroffen als Grundlage für die weitere Datenverarbeitung einholt.

Nichtsdestotrotz stellen aber über die Limitierung der Einwilligung hinaus Anpassungen im Hinblick auf die Klagebefugnis von Verbänden sowie der Transparenz der Datenverarbeitung vorteilhafte Ergänzungen im Rahmen einer Neuausrichtung des Datenschutzrechts dar.[30] Jedoch muss in diesem Zusammenhang auch bedacht werden, dass ein Ausbau an Informationspflichten nicht generell zu einer besser informierten

der Euorpäischen Union vom 15. Juni 2015, 9565/15; so auch Albrecht, CR 2016, 88 (91).

[28] Zech, WRP 2013, 1434 (1434).

[29] Spindler, GRUR-Beilage 2014, 101 (103).

[30] Zur Neuregelung des Verbandsklagerechts bei Datenschutzverstößen: Spindler, ZD 2016, 144; Ritter/Schwichtenberg, VuR 2016, 95; zur Forderung von mehr Transparenz unter anderem: Bechler, Informationseingriffe durch intransparenten Umgang mit personenbezogenen Daten, S. 194.

Einwilligung durch den Betroffenen führt, sondern auch in einen alltagsuntauglichen Formalismus münden kann. In den nächsten Jahren wird ferner davon auszugehen sein, dass das Urteil des EuGH zu Safe Harbor insbesondere die transnationale datenschutzrechtliche Debatte um die Informationsverarbeitung bei Privaten weiter prägen wird.[31]

3.6 Zwischenergebnis

Die verschiedenen Reformansätze zur Modernisierung des Rechts auf informationelle Selbstbestimmung im Internetzeitalter verdeutlichen die allgemeine Auffassung, dass der Schutz personenbezogener Daten in seiner derzeitigen rechtlichen Ausgestaltung in nicht mehr ausreichendem Maße den aktuellen technischen Anforderungen genügt. Insbesondere die veränderten Gegebenheiten für die automatisierte Datenverarbeitung im Internet und die dort angebotenen Dienste lassen sich nur schwer mit den geltenden nationalen und europäischen Vorschriften in einer Art und Weise vereinbaren, welche die Interessen aller Beteiligten in einen angemessenen Ausgleich bringt.

Bei den zur Lösung dieser Konfliktlage vorgestellten Ansätzen zeigen sich im Einzelnen Praktikabilitätsschwächen. Im Volkszählungsurteil leitete das Bundesverfassungsgericht das Recht des Einzelnen, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“,[32] aus dem Allgemeinen Persönlichkeitsrecht ab. Dies geschah zu einer Zeit, in der im Regelfall weder zur Erledigung von Einkäufen noch zum Pflegen sozialer Kontakte, geschweige denn zum Auffinden von Informationen, personenbezogene Daten an Dritte preisgegeben werden mussten. Mittlerweile jedoch hat ein beträchtlicher Teil der persönlichen Lebensgestaltung eine Ausdehnung in den digitalen Raum hinein erfahren. Diese Entwicklung hat es mit sich gebracht, dass sich personenbezogene Daten auch zum Wirtschaftsgut entwickelten und nunmehr neben ihrem ideellen persönlichkeitsrechtlichen Ursprung auch eine kommerzielle Komponente besitzen. Ein Datenschutzrecht, das zukunftsorientiert ausgestaltet ist, muss diesen beiden – nicht selten gegenläufigen – Interessen zwischen Persönlichkeitsschutz und Wirtschaftlichkeit in der Informationsverarbeitung gerecht werden. Es darf sich einerseits in seinem Wertgehalt nicht ausschließlich durch seine persönlichkeitsrechtliche Herkunft definieren, diese andererseits aber auch nicht über die Maße negieren, indem es das Recht auf informationelle Selbstbestimmung zu einem reinen Wirtschaftsrecht reduziert. Deshalb ist es zur Entwicklung eines praktikablen Datenschutzmodells notwendig, die verschiedenen Lösungsvorschläge, die für den zukünftigen Schutz der informationellen Selbstbestimmung diskutiert werden, miteinander zu kombinieren und hierdurch die unterschiedlichen Interessenlagen in Ausgleich zu bringen.

[31] Siehe EuGH Urt. v. 6.10.2015 – C-362/14, EuZW 2015, 881 – Schrems.
[32] BVerfGE 65, 1 (43); BVerfGE 63, 131 (142 f.).

4 Vorschlag zur Stärkung der informationellen Selbstbestimmung bei der Online-Datenverarbeitung: die vorformulierten Datenschutzbestimmungen

4.1 Unzulänglichkeit der AGB-Kontrolle von Datenschutzbestimmungen

Aufgrund der fehlenden Gestaltungsmöglichkeit durch den Betroffenen unterstellt die Rechtsprechung datenschutzrechtliche Einwilligungserklärungen regelmäßig der AGB-Kontrolle nach §§ 305 ff. BGB.[33] Dadurch wird der schwächeren Vertragspartei ermöglicht, auch bei umfangreichen AGB darauf zu vertrauen, dass diese keine überraschenden oder in besonderem Maße benachteiligenden, versteckten Klauseln enthalten. Dennoch trifft den Betroffenen bei einer Klage gegen die verarbeitende Stelle insoweit ein hohes Prozessrisiko, als dass, insbesondere bei den relativen Klauselverboten und der Generalklausel, das Ergebnis der Inhaltskontrolle nur schwer vorauszusehen ist. Zudem entfaltet ein etwaiges Urteil keine Wirkung gegenüber Dritten, sodass in einem zweiten Verfahren in Bezug auf dieselben AGB der Ausgang grundsätzlich offen ist. Nicht zuletzt auch angesichts der ohnehin schon sehr geringen Anreize für den Betroffenen, gegen Datenschutzverstöße vorzugehen,[34] stellt die AGB-Kontrolle im Bereich der Datenschutzbestimmungen kein zufriedenstellendes Instrument dar. Es bedarf somit spezieller Regularien, die eine effektive Kontrolle durch den Betroffenen schon im Vorfeld, das heißt bei Erteilung seiner Einwilligung, ermöglichen. Im Bereich der Datenschutzbestimmungen sollte aufgrund der vorgestellten Spezifika sowie des persönlichkeitsrechtlichen Schutzinhalts die AGB-Kontrolle deshalb einem System vorformulierter Datenschutzbestimmungen weichen. Hierdurch kann eine transparentere Einwilligungssituation geschaffen und eine schnellere sowie praktikablere Kontrolle der Datenschutzbedingungen durch den Betroffenen selbst ermöglicht werden, ohne dass erst die Gerichte im Nachgang an die Einwilligungserteilung der informationellen Selbstbestimmung zu ihrer Wirksamkeit verhelfen müssen

4.2 Die Verpflichtung zur Nutzung vorformulierter Datenschutzbestimmungen

Die Schnelllebigkeit in der Onlinewelt hat zur Folge, dass regelmäßig eine Vielzahl von Verträgen im Internet abgeschlossen wird, die in der Regel mit einer Preisgabe personenbezogener Daten einhergehen. Da es für den Einzelnen zeitlich oft unmöglich ist, alle Datenschutzbestimmungen zu lesen und zu bewerten,[35] bedarf es Instrumente, die es dem Betroffenen erleichtern, ihre Rechtskonformität selbst zu überprüfen und auf

[33] Siehe u.a. BGH GRUR 2008, 1010 (1011); LG Berlin; NJW 2013, 2605 (2606).
[34] Spiecker gen. Döhmann, in: Hain/Pfeifer (Hrsg.), Datenschutz im digitalen Zeitalter, S. 61 (76).
[35] Siehe hierzu auch Bolsinger, DuD 2016, 382 (385).

diese Weise die Ausübung seines Rechts auf informationelle Selbstbestimmung unterstützen.[36]

Die Verwendung vorformulierter Datenschutzklauseln setzt zunächst voraus, dass auf gesetzgeberischer Seite ein Katalog von Klauseln erstellt wird, die im Einklang mit nationalen und europäischen Datenschutzvorgaben stehen und die von einer verarbeitenden Stelle zur Erstellung ihrer Datenschutzbestimmungen verwendet werden. Bei den vorformulierten Klauseln handelt es sich folglich um hinreichend detaillierte positivrechtliche Vorgaben schon bei Einwilligungserteilung, die als Substitut einer nachträglichen Verbotskontrolle durch die AGB-rechtlichen Vorschriften fungieren sollen.

Aufgrund der positiven Formulierung solcher Klauseln wird es dem Betroffenen erleichtert, die Schwere eines Eingriffs in sein Recht auf informationelle Selbstbestimmung eigenständig zu überprüfen und abzuschätzen. Selbst wenn die datenverarbeitende Stelle sich bei Abruf der Einwilligung nicht an die Klauselvorgaben halten sollte, ist das Prozessrisiko des Betroffenen im Vergleich zu einer gerichtlichen Überprüfung relativer Klauselverbote oder gar nur einer Generalklausel im Rahmen von AGB deutlich geringer, da nur eine formelle Überprüfung auf die Einhaltung des Klauselkataloges hin stattfinden muss. Die Schwelle für den Einzelnen, im Zweifelsfall eine gerichtliche Überprüfung von Datenschutzbestimmungen anzustreben, wird auf diese Weise deutlich gesenkt, sodass der Vorschlag ebenfalls einen Schritt zur Bekämpfung des Vollzugsdefizits darstellt. Die Verpflichtung zur Verwendung vorformulierter Datenschutzbestimmungen hat für den Betroffenen zudem den Vorteil, dass er sich mit den Datenschutzbestimmungen für einzelne Geschäftsbereiche nur einmal auseinandersetzen muss, da für alle Dienste dieselben Klauseln gelten.

Vorformulierte Klauseln bieten zudem die Möglichkeit, Datenschutzbestimmungen übersichtlich zu gestalten, indem sie ausschweifende Formulierungen der datenverarbeitenden Stelle verhindern. Deshalb sind sie ein wichtiger Beitrag zu dem Ziel, die Verarbeitung personenbezogener Daten für den Betroffenen transparenter zu gestalten. Insoweit stellen die vorformulierten Datenschutzbestimmungen auch eine Konkretisierung des allgemeinen Transparenzgebotes nach § 4a BDSG dar, an dessen Einhaltung es in der Praxis häufig mangelt, weil die Datenschutzbestimmungen letztlich frei vom Datenverarbeiter festgelegt werden.[37] Ebenso sind die fest vorgegebenen Klauseln dazu geeignet, weitere datenschutzrechtliche Grundsätze wie das Zweckbindungsprinzip oder den Bestimmtheitsgrundsatz konkret und für den Einwilligenden sowohl verständlich wie auch kontextbezogen wiederzugeben.

Das soziale Netzwerk Instagram hält sich beispielsweise in seinen Datenschutzrichtlinien die Möglichkeit vor, nach der Schließung oder Deaktivierung des

[36] Neben Ansätzen, die – wie in diesem Beitrag vorgeschlagen – den Inhalt der Einwilligungserklärung betreffen, sind auch Vorschläge, die dem Betroffenen eine visuelle Unterstützung bieten, vorstellbar, siehe dazu Pollmann/Kipker, DuD 2016, 378.

[37] Gola/Klug/Körffer, in: Gola/Schomerus, BDSG, § 4a Einwilligung, Rn. 23.

Kontos Informationen und Nutzerinhalte „für einen kaufmännisch angemessenen Zeitraum für Backup-, Archivierungs- bzw. Prüfzwecke“ aufzubewahren.[38] Für einen Privatnutzer ist aus dieser Klausel nicht erkennbar, mit welcher auch nur ungefähren Speicherungsdauer er zu rechnen hat und was konkret unter Archivierungs- und Prüfzwecken verstanden werden kann. Verstöße gegen das Transparenzgebot und den Bestimmtheitsgrundsatz liegen deshalb nahe. Letzterer verlangt, dass sich die Einwilligung auf einen genau umschriebenen Verwendungsvorgang bezieht, pauschal gehaltene Erklärungen bzw. nur allgemeine Angaben können deshalb nicht ausreichend sein.[39] Ein Verstoß gegen das Transparenzgebot ergibt sich ferner aus Art. 13 Abs. 2 der neuen EU-Datenschutzgrundverordnung, wonach die Angabe der Speicherungsdauer oder Kriterien für deren Festlegung eine notwendige Information darstellt, um eine transparente Datenverarbeitung zu gewährleisten. Eine vorformulierte Datenschutzklausel könnte unter diesen Gesichtspunkten eine maximale Speicherungsdauer festlegen oder eine Auswahl konkreter Kriterien zur Festlegung der Dauer bestimmen. Daneben ist es möglich, die Verwendungszwecke von Anfang an hinreichend konkret zu fassen, indem die für die Archivierung und Prüfung notwendigen Verarbeitungsvorgänge weiter aufgeschlüsselt werden.

Die vorformulierten Datenschutzbestimmungen bieten ferner den Vorteil einer leichten Überprüfbarkeit der Rechtslage, denn durch den Ausschluss individueller Klauseln des einzelnen Datenverarbeiters wird dem Betroffenen eine Sicherheit dahingehend gegeben, dass er von der Unwirksamkeit solcher Datenschutzbestimmungen ausgehen kann, die nicht mit den vorformulierten Klauseln konform sind. In diesem Zusammenhang bietet sich eine technisch verhältnismäßig leicht implementierbare Überprüfungsmöglichkeit über einen automatisierten Textabgleich der verwendeten Klauseln mit den offiziellen, von staatlicher Seite aus bestimmten Vorgaben für ein bestimmtes Geschäftsmodell an, die beispielsweise auf behördlichen Websites zum Download zur Verfügung stehen. Eine Aufsplittung der Klauselvorgaben nach unterschiedlichen Geschäftszwecken ist auch deshalb sinnvoll, weil in jeder datenverarbeitenden Branche mit verschiedenen Verarbeitungsszenarien zu rechnen ist. So ist es vorstellbar, unterschiedliche Bestimmungen zum Beispiel für soziale Netzwerke, E-Commerce-Unternehmen, Informationsdienste und Online Games zu schaffen. Insbesondere wird auch davon auszugehen sein, dass sich die spezifischen Anforderungen an eine Datenerhebung und -verarbeitung innerhalb einer bestimmten Branche bzw. eines Geschäftsmodells nur in geringfügigem Maße unterscheiden, sodass kein Bedarf besteht, die vorformulierten Datenschutzbestimmungen um individuelle Klauseln zu ergänzen.[40] Systematisch sind die Klauselvorgaben in der Form eines Baukastens zu fassen, aus welchem sich der Datenverwender entsprechend seinen Anforderungen die jeweiligen Bestimmungen

[38] https://de-de.facebook.com/help/instagram/155833707900388/.

[39] Simitis, in: Simitis, BDSG, § 4a, Rn. 77 ff.

[40] Beispielsweise zeigt ein Vergleich der Online-Games-Anbieter Europe Entertainment Ltd. und upjers GmbH, dass die Datenverwendungszwecke beider Anbieter grundsätzlich übereinstimmen; sie bestehen im Wesentlichen in der Bereitstellung und Gewährleistung des Spielbetriebs, der Zahlungsabwicklung, von Kundenserviceleistungen und in der Datenverarbeitung zu Marketingzwecken; siehe https://www.stargames.net/de/allgemeine-geschaeftsbedingungen#privacy, https://de.upjers.com/privacy.

auswählen und zu seinen individuellen Datenschutzbestimmungen zusammenstellen kann. Dadurch wird insbesondere auch solchen Anbietern Rechnung getragen, die eine Kombination verschiedener Dienste anbieten und sich keinem Geschäftsmodell alleinig zuordnen lassen. Freilich muss der Anbieter in überprüfbarer Weise kenntlich machen, innerhalb welcher Branchen er tätig ist, um eine Verwendung der vorformulierten Klauseln über das benötigte Maß hinaus zu vermeiden. Denkbar wäre hier eine Registrierung der Geschäftskategorien bei den Datenschutzbehörden. Diesen ohnehin schon überlasteten Einrichtungen wird es durch systematisch kategorisierte wie vorformulierte Klauseln zudem erleichtert, Bestimmungen einzelner Anbieter im Zweifelsfall – beispielsweise nach Anrufung durch einen Nutzer – zu überprüfen und zu bewerten.

Sämtliche Einwilligungserteilungen im Rahmen der vorformulierten Datenschutzbestimmungen haben denknotwendigerweise als Opt-in zu erfolgen. Dies allein schon deshalb, weil die Europäische Datenschutzgrundverordnung fußend auf Art. 4 Nr. 11 dem Opt-out-Modell jegliche gesetzliche Grundlage entzogen hat.

5 Fazit und Ausblick

Die informationelle Selbstbestimmung steht im Onlinezeitalter vor erheblichen Herausforderungen. Damit sie im Informationsalltag nicht leerläuft, bedarf es neuer Regelungsmechanismen. Dazu werden verschiedene Konzepte vertreten. Die Einführung vorformulierter Datenschutzbestimmungen stellt einen praktisch ausgerichteten Lösungsansatz dar. Indem durch ihre Verwendung die maßgeblichen, aber für den täglichen Gebrauch zu abstrakt gefassten Grundsätze des Datenschutzes in eine konkrete Form gegossen werden, können die Klauseln ein wesentliches Instrument sein, um die datenschutzrechtliche Einwilligung zukunftsfest zu machen.

Literaturverzeichnis

[Bä12] Bäcker, Matthias: Grundrechtlicher Informationsschutz gegen Private. Der Staat 51/12, S. 91-116, 2012.

[Be10] Bechler, Lars: Informationseingriffe durch intransparenten Umgang mit personenbezogenen Daten. Universitätsverlag Halle-Wittenberg, Halle (Saale) 2010.

[Bo16] Bolsinger, Harald: Wo bleibt die digitale Dividende für Europas Konsumenten?. Datenschutz und Datensicherheit 06/16, S. 382-385.

[Br10] Britz, Gabriele: Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts. In (Hoffmann-Riem): Offene Rechtswissenschaft, S. 561-596, Mohr Siebeck Verlag, Tübingen 2010.

[Bu15] Buchner, Benedikt: Message to Facebook. Datenschutz und Datensicherheit 06/15, S. 402-405, 2015.

[Bu14] Buchner, Benedikt: Facebook zwischen BDSG und UWG. In (Alexander/Bornkamm/Buchner/Fritz, Hrsg.): Festschrift für Helmut Köhler zum 70. Geburtstag, S. 51-62, C.H. Beck Verlag, München 2014.

[Bu06] Bull, Hans Peter: Zweifelsfragen um den informationellen Selbstbestimmung-Datenschutz als Datenaskese?. Neue Juristische Wochenschrift 23/06, S. 1617-1624, 2006.

[GKK15] Gola, Peter; Schomerus, Rudolf: Bundesdatenschutzgesetz, Kommentar, 12. Auflage, C.H. Beck Verlag, München 2015.

[Gi14] Giesen, Thomas: Für ein verfassungsgemäßes Datenschutzrecht in Europa. Computer und Recht 08/14, S. 550-556, 2014.

[Gr13] Grimm, Dieter: Der Datenschutz vor einer Neuorientierung. JuristenZeitung 12/13, S. 585-592, 2013.

[Hä12] Härting, Niko: Datenschutz und Persönlichkeitsrechte: Verbotsprinzip und offener Tatbestand. In (Leible/Kutschke, Hrsg.): Der Schutz der Persönlichkeit im Internet, S. 55-64, Boorberg Verlag, Stuttgart 2013.

[Hä13] Härting, Niko: Anonymität und Pseudonymität im Datenschutzrecht. Neue Juristische Wochenschrift 29/13, S. 2065-2071, 2013.

[Ho98] Hoffmann-Riem, Wolfgang: Informationelle Selbstbestimmung in der Informationsgesellschaft. Archiv des öffentlichen Rechts Band 123/98, S. 513-540, 1998.

[Ki14] Kilian, Wolfgang: Strukturwandel der Privatheit. In (Garstka/Coy, Hrsg.): Wovon-für wen-wozu-Systemdenken wider die Diktatur der Daten, S. 195-224, Berlin, 2014.

[Ma12] Masing, Johannes: Herausforderungen des Datenschutzes. Neue Juristische Wochenschrift 32/2012, S. 2305-2311, 2012.

[Pl13] Plath, Kai-Uwe: Kommentar zum BDSG sowie den datenschutzrechtlichen Regelungen des TMG und des TKG. Otto Schmidt Verlag, Köln 2013.

[PK16] Pollmann, Maren; Kipker, Dennis-Kenji: Informierte Einwilligung in der Online-Welt. Datenschutz und Datensicherheit 06/16, S. 378-381, 2016.

[Re15] Reiners, Wilfried: Datenschutz in der Personal Data Economy-Eine Chance für Europa. Zeitschrift für Datenschutz 02/15, S. 51-55, 2015.

[RS16] Ritter, Franziska; Schwichtenberg, Simon: Die Reform des UKlaG zur Eliminierung des datenschutzrechtlichen Vollzugsdefizits – neuer Weg, neue Chancen?. Verbraucher und Recht 03/16, S. 95-102, 2016.

[Sc11] Schneider, Jochen: Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip. AnwaltsBlatt 04/11, S. 233-239, 2011.

[Sc12] Schoch, Friedrich: Das Recht auf informationelle Selbstbestimmung in der Informationsgesellschaft. In (Sachs/Siekmann, Hrsg.): Der grundrechtsgeprägte Verfassungsstaat – Festschrift für Klaus Stern zum 80. Geburtstag, S. 1491-1512, Duncker & Humblot, Berlin 2012.

[Se14] Seidel, Ulrich: Das Grundrecht auf Datensouveränität. Zeitschrift für Gesetzgebung 29/14, S. 153-165, 2014.

[Si14] Simitis, Spiros: Kommentar zum Bundesdatenschutzgesetz. 8. Auflage, Nomos-Verlag, Frankfurt a.M. 2014.

[Sp13] Spiecker gen. Döhmann: Die Durchsetzung datenschutzrechtlicher Mindestanforderungen bei Facebook und anderen Sozialen Netzwerken – Überlegungen zu Vollzugsdefiziten im Datenschutzrecht. In (Leible/Kutschke, Hrsg.): Der Schutz der Persönlichkeit im Internet, S. 33-54, Boorberg, Stuttgart 2013.

[Sp15] Spiecker gen. Döhmann: Zur Architektonik des europäischen und deutschen Datenschutzes im Zeitalter von Vorratsdatenspeicherung, Big Data und IT-Enhancement im Lichte der *Google Spain*-Entscheidung des *Europäischen Gerichtshofs*. In (Hain, K.-E./Pfeifer, N. Hrsg.): Datenschutz im digitalen Zeitalter – global, europäisch, national, S. 61-91, C.H. Beck Verlag, München 2015.

[Sp14] Spindler, Gerald: Datenschutz und Persönlichkeitsrechte im Internet. Gewerblicher Rechtsschutz und Urheberrecht – Beilage 01/14, S. 101-108, 2014.

[Sp16] Spindler, Gerald: Verbandsklagen und Datenschutz – das neue Verbandsklagerecht. Zeitschrift für Datenschutz 03/16, S. 114-119, 2016.

[Ze13] Zech, Herbert: Durchsetzung von Datenschutz mittels Wettbewerbsrecht?. Wettbewerb in Recht und Praxis 11/13, 1434-1436, 2013.