Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 1061

Herausforderungen bei der Entwicklung von Anwendungen zum Selbstdatenschutz

Sascha Alpers[1], Maria Pieper[1] und Manuela Wagner[2]

Abstract: Durch zunehmende Vernetzung steigt die Notwendigkeit, Betroffene in der Ausübung ihres Privatsphärenschutzes zu unterstützen. Wenn technische Lösungen dabei in die Integrität urheberrechtlich geschützter Computerprogramme eingreifen oder Geschäftsmodelle „Dienst gegen Daten" vereiteln, stellt sich die Frage der urheber- und lauterkeitsrechtlichen Bewertung im Spannungsverhältnis zum Selbstdatenschutz. In diesem Beitrag werden die rechtlichen Herausforderungen, auch im Hinblick auf aktuelle Vorschläge der Datenökonomisierung, beleuchtet und mit einem Exkurs zu den Anforderungen der intelligenten Bereitstellung generierter Daten zur Verschleierung persönlicher Informationen abgeschlossen.

Keywords: Selbstdatenschutz, Bearbeitungsrecht, Wettbewerbsbehinderung

1 Einleitung

Die Digitalisierung des Alltags erfordert technische Unterstützung zum Selbstdatenschutz, um für Betroffene den Aufwand des Privatsphärenschutzes handhabbar zu gestalten. Obwohl Bürgerbefragungen die Skepsis gegenüber datengetriebenen Geschäftsmodellen aufzeigen [Bi16], geben Nutzer gegenüber unterschiedlichen Diensten ihre Daten preis. (Ein Indiz für dieses widersprüchliche Nutzerverhalten ist bspw. der wachsende Big-Data-Wirtschaftssektor.[3]) Dieses Privacy-Paradoxon [No07] könnte u. a. mit dem Aufwand Privatsphärenrisiken adäquat einzuschätzen oder der Schwierigkeit privatsphärenschützende Alternativen zu nutzen, zusammenhängen [Wh14, S. 14 f.]. Daher dürfte der Erfolg von Datenschutzlösungen auch von der Usability abhängen. Da ein Wechsel zu datenschutzfreundlichen Angeboten aufgrund von Netzwerkeffekten [We11] oft mit Einbußen (z. B. digitaler Isolation) verbunden ist, sollen Selbstdatenschutzlösungen die Teilhabe am digitalen sozialen und kulturellen Leben ermöglichen, ohne auf Privatsphärenschutz verzichten zu müssen. Hierbei können Filtermechanismen die rechtswidrige Weitergabe personenbezogener Daten Dritter[4] unterbinden.

Die europäische Datenschutzgrundverordnung (DSGVO) enthält die Verpflichtung zu Pri-

[1] FZI Forschungszentrum Informatik, Forschungsbereich Software Engineering, Haid- und Neustraße 10–14, 76131 Karlsruhe, {alpers | pieper}@fzi.de.
[2] Karlsruher Institut für Technologie, Zentrum für Angewandte Rechtswissenschaft, Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe, manuela.wagner@kit.edu.
[3] Der Big-Data-Sektor wächst um 40 % pro Jahr, sieben Mal schneller als der gesamte IT-Markt [Be17, S. 6].
[4] Die Preisgabe von Kontaktdaten Dritter ohne Einwilligung wurde jüngst als deliktische Handlung eingestuft, siehe AG Bad Hersfeld, Beschluss vom 15. Mai 2017 – F 120/17 EASO.

doi:10.18420/in2017_108

vacy by Design und by Default sowie Datenminimierung. Zur Umsetzung datenschutzfreundlicher Voreinstellungen sollten Anbieter von Smartphone-Apps ein dynamisches Datenzugriffsmanagement bereitstellen, um die Datenzugriffe auf das je nach individueller Nutzung notwendige Maß einzuschränken. Im Konflikt hierzu stehen jedoch „Alles-oder-Nichts-Lösungen", bei denen die Abfrage personenbezogener Daten über die Diensterbringung hinaus der Refinanzierung des Angebots dient. Solange Einstellungsmöglichkeiten zur individuellen Datenzugriffseinschränkung noch nicht die Regel sind und Privatnutzern das technische Know-how für effektiven Selbstschutz fehlt, stellt die Entwicklung von Selbstdatenschutzanwendungen eine sinnvolle Möglichkeit dar, privatsphärenschützende Einstellungen technisch durchzusetzen. Zu den technischen Herausforderungen gehören die plattform- und dienstübergreifende Durchsetzung des Selbstdatenschutzes und die damit verbundene Vielzahl an plattform- und dienstspezifischen Schnittstellen. Eine weitere Herausforderung ist die Heterogenität der schützenswerten Daten. Hierzu zählen bspw. Adressbuch und Kalendereinträge, Standortdaten sowie Gesundheitsdaten. In rechtlicher Hinsicht ist das Spannungsverhältnis widerstreitender Grundrechte zu bedenken.[5] Dieser Beitrag widmet sich dem Konflikt zum Urheberschutz von Computerprogrammen sowie technischen Lösungsansätzen (Abschnitt 2). Der Fokus liegt hierbei auf dem Eingriff in die Datenkommunikation. Es werden auch mögliche Implikationen der Datenzugriffsblockade im Zusammenhang mit den aktuellen Diskussionen um die rechtliche Anerkennung von Geschäftsmodellen „Dienst gegen Daten" in Bezug auf den Schutz vor unlauterem Wettbewerb aufgezeigt (Abschnitt 3). Abschließend erfolgt ein Exkurs, der eine Selbstdatenschutzlösung mittels Generierung von falschen Daten und daran anknüpfende rechtliche und technische Anforderungen (Abschnitt 4) skizziert.

2 Selbstdatenschutz im Konflikt mit Urheberrechten?

Einige technische Lösungen unterstützen den Betroffenen beim Selbstdatenschutz. Eine konkrete Analyse am Markt befindlicher Selbstdatenschutzlösungen findet sich in [Al16]. Abb. 1 stellt die gängigen Ansätze gegenüber. Dabei sind Ergänzungen oder Veränderungen an bestehenden Komponenten dunkelblau hervorgehoben. Einige Lösungen entfernen ungewollte Berechtigungen aus der Manifestdatei[6] der zu kontrollierenden App (Abb. 1, li.). Andere Lösungen fügen der App eine eigene Sicherheitsbibliothek hinzu und müssen dazu i. d. R. auch den existierenden Programmcode anpassen, um die Verwendung der Bibliothek zu erzwingen (Abb. 1, Mitte. Blaue Kreise repräsentieren Anpassung am bestehenden Code.). Auch die Veränderung des Betriebssystems ist eine gängige Lösungsstrategie, sodass unerwünschte App-Zugriffsanfragen nicht positiv beantwortet werden (Abb. 1, re.). Sowohl für den zweiten als auch für den dritten Fall werden sog. Sandboxes

[5] Die Durchsetzung des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs.1, 1 Abs. 1 GG) bzw. des Rechts auf Achtung des Privat- und Familienlebens sowie Schutz personenbezogener Daten nach Art. 7, 8 EU-GrundrechteCharta (EU-GrCh) kann insbesondere im Konflikt mit der Berufs- und Eigentumsfreiheit (Art. 12, 14 GG bzw. Art. 15, 16, 17 EU-GrCh) der App-Anbieter stehen.

[6] Teil des Installationspakets einer Anwendung, enthält u. a. Informationen zu angeforderten Berechtigungen einer Anwendung.

eingesetzt. Als Sandbox wird dabei eine Umgebung bezeichnet, welche die Aktionen einer Anwendung gemäß definierter Regeln einschränkt [Bi03]. Durch diese Zugriffsbeschränkung wird das Risiko einer Verletzung der definierten Regeln reduziert [Go96]. Das Konzept stammt aus der IT-Sicherheit, lässt sich aber auf den Selbstdatenschutz übertragen. Soweit diese Lösungen Programmcode verändern, entsteht ein Konflikt zwischen dem Interesse eines umfassenden Privatsphärenschutzes und dem Schutz von Computerprogrammen als geistiges Eigentum.

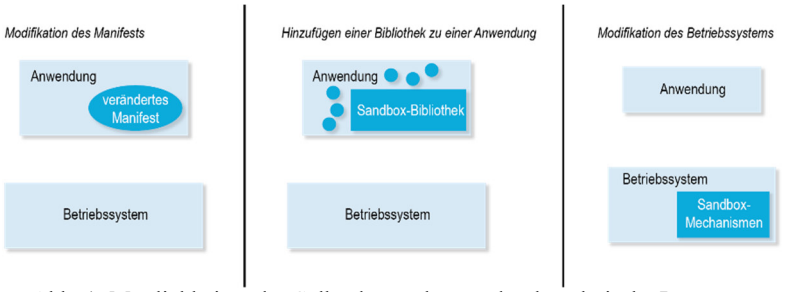

Abb. 1: Möglichkeiten des Selbstdatenschutzes durch technische Lösungen

2.1 Verändern der Programmsubstanz

Computerprogramme sind nach § 69a UrhG geschützt, wenn sie das Ergebnis einer eigenen menschlich-schöpferischen Tätigkeit sind, die einen geistigen Gehalt aufweist und eine ausreichende individuelle, gestalterische Schöpfungshöhe erreicht [DS15, § 69a Rn. 26]. Der Begriff ist weit zu verstehen und kann auch Hilfsprogramme, Programmteile und Schnittstellen umfassen [DS15, § 69a Rn. 12]. Ein eigenständiger Schutz der Manifestdatei erscheint zweifelhaft, da Einträge oft automatisch erfolgen.[7] Über die Eintragslöschung könnte jedoch eine dem Urheber vorbehaltene Umarbeitung der Gesamtanwendung i. S. d. § 69c Nr. 2 UrhG vorliegen. Versteht man ein Computerprogramm als „eine zur Lösung einer Aufgabe vollständige Anweisung, zusammen mit allen erforderlichen Vereinbarungen“[8], ist die Einschränkung oder Ergänzung des Funktionsumfangs durch Entfernung oder Hinzufügen von Programmteilen eine Umarbeitung [Bo13, S. 722]. Das Löschen von Teilen der Manifestdatei oder Hinzufügen einer Sicherheitsbibliothek ist eine Veränderung der Programmsubstanz. Auch Umarbeitungen des jeweiligen Betriebssystems sind lizenzpflichtig, einige Open-Source-Lizenzen erlauben die Bearbeitung [Br14a, S. 547 f.].

[7] Bei autonom generierten Computerprogrammen wird auf die Entwicklung des Ursprungsprogramms zurückgegriffen [DS15, § 69a Rn. 26). Dieses dürfte sich im vorliegenden Fall jedoch eher an der Funktionalität orientieren. Routinemäßig und von einer Vielzahl von Programmierern allgemein genutzte Programmbestandteile sind nicht schutzfähig, solange sich die Gestaltung aus der Natur der Aufgabe und aus rein funktionalen Erwägungen ergibt [DS15, § 69a Rn. 27].

[8] [DS15, § 69a Rn. 12] mit Verweis auf DIN 44 300.

2.2 Eingriff in den Programmablauf

Nach einer Entscheidung des OLG Hamburg soll eine Umarbeitung auch bei einer Veränderung des Programmablaufs vorliegen, ohne dass eine permanente Veränderung der Programmsubstanz selbst erfolgt.[9] Da die Gliederung des Programmablaufs, Anordnung der Programmelemente sowie deren Zusammenwirken geschützt sind[10], könne auch eine externe Software, die „im Ergebnis einen Teil der Steuerung übernimmt", die Ablaufroutine in einer vom Urheber nie vorgesehenen Weise verändern.[11] Die Anpassung an individuelle Benutzerwünsche oder Erweiterungen des Funktionsumfangs stelle eine lizenzpflichtige Umarbeitung dar, da dem Urheber das Customizing zusteht.[12] Das Einspielen „falscher" Daten sei dagegen zulässig, solange die Daten keine Befehle enthalten, die das geschützte Programm kontrollieren oder steuern.[13] Lösungsansätze, die zwar den Code nicht verändern, müssten demnach prüfen, ob die Unterbindung der Datenkommunikation zwischen App und Betriebssystem lediglich als Einspielen „falscher Daten" oder als Eingriff in den Programmablauf zu werten wäre.

Gegen diese weite Interpretation wurde eingewandt, dass die Funktion einer Software nicht vom Urheberrecht geschützt wird [Sp12, S. 417]. In der Nichtansteuerung bestimmter Programme liege lediglich ein Eingriff in deren nach außen in Erscheinung tretende Funktion.[14] Eine zu weite Interpretation der Bearbeitung dürfe nicht die Nutzung vorhandener Schnittstellen unterbinden und die Interoperabilität und Interaktion verschiedener Programme gefährden.[15] Der Schutz vor Umarbeitung rechtfertige es nicht, temporäre Einwirkungen, wie das Unterdrücken von Programmteilen, zu verbieten.[16] Solange eine Einschränkung des Funktionsumfangs nicht durch einen Eingriff in die im Code verkörperte Folge von Befehlen als Schutzgegenstand des § 69a UrhG erfolgt, d. h. ein Eingriff in die Programmsubstanz gegeben ist, läge keine lizenzpflichtige Umarbeitung vor.[17] Dem ist zuzustimmen, da andernfalls die Interaktion verschiedener Programme gefährdet wäre.

2.3 Zulässigkeit von Umarbeitungen

Dienen Codemanipulationen der bestimmungsgemäßen Nutzbarmachung des Computerprogramms, wie die Fehlerberichtigung, sind diese ohne Zustimmung des Urhebers zulässig (§ 69d Abs. 1 UrhG). Zur Ermöglichung einer rechtmäßigen Nutzung könnte die Abwehr rechtswidriger Datenzugriffe als Form der „Mängelbeseitigung" hierunter fallen [Bo13, S. 725], [Br14a, S. 545]. Hierin könnte ein Ausgleich zwischen Daten- und immateriellen Eigentumsschutz gesehen werden. Die Datenschutzkonformität unterliegt jedoch

[9] OLG Hamburg, Urteil vom 13.04.2012 – 5 U 11/11, GRUR-RR 2013, 13, 15 – „*Replay PSP*".
[10] KG Berlin, Urteil vom 17. März 2010 – 24 U 117/08.
[11] OLG Hamburg, (Fn. 9).
[12] OLG Hamburg, (Fn. 9).
[13] OLG Hamburg, Urteil vom 12.03.1998 – 3 U 226/97; OLG Düsseldorf, Urteil vom 12.7.1999 – 20 U 40/99.
[14] Vgl. KG Berlin, Urteil vom 06. September 2010 – 24 U 71/10.
[15] LG Hamburg, Urteil vom 03.05.2016 – 308 O 46/16– Rn. 28.
[16] LG München I, Urteil vom 27. Mai 2015 – 37 O 11673/14 –, Rn. 289.
[17] LG Hamburg, (Fn. 15); LG München I, (Fn. 16).

der Einzelfallprüfung. Dem Nutzer würde das Risiko auferlegt, die Rechtskonformität der App eigenverantwortlich zu prüfen. Für eine umfassende technische Lösung müsste das Recht auf informationelle Selbstbestimmung ein Recht zur (Mit-)Inanspruchnahme von datenschutzkonformen Anwendungen umfassen. Ein prinzipieller Vorrang grundrechtlich geschützter Rechte ist der Verfassung eher fremd, der Ausgleich widerstreitender Freiheitsrechte erfolgt nach dem Grundsatz der Verhältnismäßigkeit im Einzelfall [Le16, S. 775]. Daher dürfte sich ein generelles Recht zur Modifikation fremder Programme kaum über § 69d Abs. 1 UrhG rechtfertigen lassen. Selbst bei weiter Auslegung verbleiben Zweifel, wenn dadurch die Funktionsfähigkeit der App beeinträchtigt wird – die „bestimmungsgemäße Benutzung" wäre dann gerade nicht hergestellt. Selbstdatenschutzlösungen sollten daher keine Umarbeitung erfordern, um ohne urheberrechtliche Bedenken für sämtliche Apps eines Nutzers angewandt werden zu können.

2.4 Lösungskonzept

Aufbauend auf vorherigen Überlegungen wird nun in Abb. 2 ein Lösungsansatz, bestehend aus einer Sandbox und einem „Reference Monitor" beschrieben.[18] Die Sandbox dient dazu, Anwendungen zu zwingen, ihre Anfragen nicht direkt an das Betriebssystem zu stellen, sondern hierfür den Reference Monitor zu nutzen.

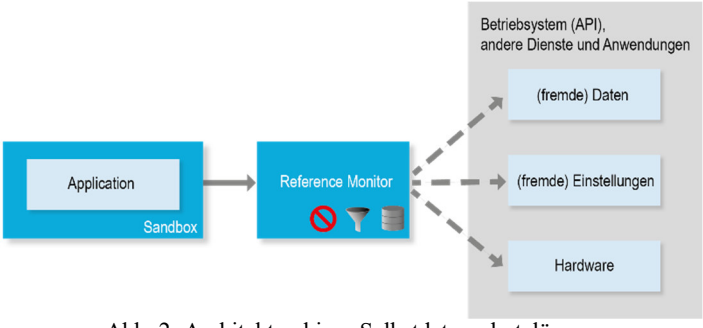

Abb. 2: Architekturskizze Selbstdatenschutzlösung

Diese Sandbox-Implementierung verändert den Code der bestehenden Anwendung nicht, sondern führt diese Anwendung in einer kontrollierten Umgebung aus. Der Reference Monitor ist die zentrale Komponente der Selbstdatenschutzlösung und dient dazu, die Einstellungen des Betroffenen hinsichtlich des dynamischen Datenzugriffsmanagements umzusetzen.[19] Dabei soll der Reference Monitor API-Aufrufe nicht nur gestatten oder blockieren können, sondern auch in der Lage sein, Antworten zu filtern. So kann bspw. bei einer Anfrage hinsichtlich des Adressbuchs nur ein Teil der Adressen (horizontaler Filter) oder nur ein Teil der Attribute (vertikaler Filter) an die anfragende Anwendung zurückgeliefert werden. Dadurch ist es bspw. möglich, die Bekanntschaft zu bestimmten Personen

[18] Ein „Reference Monitor" ist ein Konzept aus der Zugriffskontrolle, das die Zugriffsanfragen aller Subjekte für alle Objekte kontrolliert [Bi03].
[19] Somit werden Urheberrechte Dritter (Anwendung und OS) nicht verletzt, siehe 2.1 und 2.2.

vor Anwendungen zu verbergen oder die Geburtsdaten aller im Adressbuch gespeicherten Personen vor einer Anwendung zu schützen.

3 Selbstdatenschutz im Konflikt mit Lauterkeitsrecht?

Die Begrenzung von Datenzugriffen steht grundsätzlich im Spannungsverhältnis zu datengetriebenen Geschäftsmodellen, die Nutzerdaten zur Refinanzierung oder Leistungserbringung benötigen. Der Vertrieb von Selbstdatenschutzlösungen könnte die Entfaltungsmöglichkeit von Wettbewerbern beeinträchtigen. Kann das konkret beanstandete Wettbewerbsverhalten andere im Absatz behindern oder stören, stellt sich die Frage, ob eine über den gewöhnlichen Leistungswettbewerb hinausgehende unlautere Beeinträchtigung vorliegt.[20] An das Bestehen eines konkreten Wettbewerbsverhältnisses sind dabei keine hohen Anforderungen geknüpft, insbesondere muss keine Branchenidentität vorliegen.[21] Eine Wettbewerbsbehinderung kann auch mittelbar durch die Mitwirkung der Nutzer erfolgen, wenn die Markttätigkeit in Verdrängungsabsicht erfolgt oder „dazu führt, dass die beeinträchtigten Mitbewerber ihre Leistung am Markt durch eigene Anstrengung nicht mehr in angemessener Weise zur Geltung bringen können".[22] Bei der Gesamtschau sind die Interessen der Mitbewerber, Verbraucher und sonstiger Marktteilnehmer sowie der Allgemeinheit mit einzubeziehen.[23] Fälle einer gezielten Behinderung können in der Umgehung technischer Schutzmaßnahmen oder der Verleitung zum Vertragsbruch liegen.[24]

3.1 Verleiten zum Vertragsbruch bei Daten als Gegenleistung digitaler Dienste?

Der Vorschlag der DInhRL-E[25] soll eine rechtliche Basis für die Verwendung personenbezogener Daten als Gegenleistung bspw. für die App-Nutzung schaffen. Die vertragstypologische Einordnung des App-Vertrags ist besonders bei vermeintlich kostenlosen Angeboten umstritten. Teils wird aufgrund der unentgeltlichen Natur trotz Fehlens eines altruistischen Interesses von einem Schenkungsvertrag ausgegangen [Kr11, S. 771] a. A. [DK17]. Entsprechend der tatsächlichen Gegebenheiten wird vertreten, man könne ein synallagmatisches Austauschverhältnis im Sinne eines Tauschvertrags annehmen [Br14b]. Dieses könnte sich auf die Erklärung der datenschutzrechtlichen Einwilligung beziehen [Bu10, S. 40]. Ein Abweichen von der vertraglich geschuldeten Hauptleistung müsste in diesem Fall Regressansprüche der Gegenseite verursachen. Daher stellt sich die Frage, ob

[20] BGH, Urteil vom 12.01.2017 – I ZR 253/14 „*World of Warcraft II*"; BGH, Urteil vom 24.06.2004 – I ZR 26/02 „*Werbeblocker*".
[21] BGH, Urteil vom 24.06.2004 – I ZR 26/02 „*Werbeblocker*". OLG Köln, Urteil vom 24.06.2016 – I-6 U 149/15 „*Adblock Plus*"; LG München, Urteil vom 22.03.2016 – 33 O 5017/15.
[22] BGH, (Fn.20).
[23] BGH, (Fn.2020); BGH, Urteil vom 17.05.2001 – I ZR 216/99 „*Mitwohnzentrale.de*".
[24] § 4 Nr. 4 UWG, BGH, (Fn.21, 21).
[25] Kommissionsentwurf einer Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte (COM 2015/634), final vom 09.12.2015.

der Einsatz personenbezogener Daten als Ware mit dem Grundrechtsschutz vereinbar ist.

Die Schaffung eines „Dateneigentums“ als ein Ausschließlichkeitsrecht des „Datenerzeugers“ wird zwar diskutiert, personenbezogene Daten müssen jedoch hiervon ausgeklammert werden [Bu17, S. 13]. Personenbezogene Daten sind als Ausfluss des Persönlichkeitsrechts selbst bei Anerkennung ideeller und materieller Bestandteile des Persönlichkeitsrechts nicht übertragbar, da die vollständige Entäußerung sämtlicher Rechte an persönlichen Daten mit dem im Recht auf informationelle Selbstbestimmung innewohnenden Menschenwürdekern unvereinbar wäre [Sp17, S. 106 ff.]. Zwar wird angenommen, dass über die Bemessung der Daten als geldwerte Gegenleistung die Partizipation der Betroffenen an den Gewinnen ermöglicht und damit der Schutz der Betroffenen verbessert würde [Se14, S. 158]. Es kann jedoch konstatiert werden, dass Nutzer für die Preisgabe ihrer Daten vor allem aufgrund von Informationsasymmetrien und Verhandlungsungleichgewichten zwischen Privatpersonen und weltweit operierenden Oligopolen keine gleichwertige Gegenleistung erhalten [HG15, S. 270 f.]. Die Schaffung eines Dateneigentums dürfte diese Ungleichgewichte nicht aufheben, sondern vielmehr Datenverwertern eine gesicherte Rechtsposition ermöglichen.

DInhRL-E sieht einen schuldrechtlichen Vertrag über Daten als Gegenleistung vor (ohne Anerkennung eines „Dateneigentums“), soweit diese aktiv durch den Verbraucher bereitgestellt werden – nicht hingegen bei passiver Preisgabe.[26] Unabhängig von der Frage, ob die aktive Eingabe ein angemessenes Anknüpfungskriterium für die Anwendbarkeit darstellen kann, bestehen gravierende Widersprüche zur DSGVO. Dies könnte zur Inkonsistenz des Rechtsrahmens führen [Op17, S. 8 f.]. Eine schuldrechtliche Bindung steht im Konflikt mit dem Widerruf der Einwilligung, der jederzeit möglich sein sollte, ohne dass der Betroffene hierdurch Nachteile befürchten muss [Hä16, S. 738]. Nach DInhRL-E soll die Vertragsbeendigung nur im Fall der Vertragswidrigkeit möglich sein. Vertragsauflösung und Rückabwicklung könnten einen Nachteil darstellen. Zudem besteht ein Widerspruch zum Kopplungsverbot in Art. 7 Abs. 4 DSGVO [Hä16, S. 738]. Teils wird diese Regelung trotz des unklaren Wortlauts in Zusammenschau mit den Erwägungsgründen 42, 43 als absolutes Kopplungsverbot verstanden, sodass im Rahmen eines Vertragsverhältnisses eine Einwilligung in zweckfremde Datenverarbeitung stets unfreiwillig und damit unwirksam wäre [AJ17, S. 70], [Da16, S. 311]. Dagegen wird vertreten, es handele sich lediglich um eine Subsumtionsanleitung für das Merkmal „freiwillig“, die nicht zu einem mittelbaren Kontrahierungszwang führen dürfe, sodass auch Dienst-gegen-Daten-Modelle bei ausreichender Transparenz möglich wären, so *Schulz* in [Go17, § 7 Rn. 23 ff.]. Echte Wahlfreiheit besteht jedoch nur dann, wenn gleichwertige Alternativen angeboten werden. Obwohl vielfach von Daten als neuer Währung gesprochen wird [Jö16], dürfte nicht allen Nutzern bewusst sein, ob und welche Daten als Gegenleistung dienen. Zwar wussten 47 bis 76 % der Teilnehmer einer Studie, dass sie mit Daten „bezahlen“, die Mehrheit erteilte hierzu jedoch selten oder nie ihre Zustimmung [Di14, S. 11, 16]. Dieses grobe Bewusstsein dürfte keinesfalls als Rechtsbindungswille gewertet werden, insbesondere wenn es

[26] Vgl. Erwägungsgrund 14 DInhRL-E, ebenso sollen Daten nach § 3 Abs. 4 S. 1 DInhRL-E keine Gegenleistung darstellen, die für die Erfüllung des Vertrags oder rechtlicher Pflichten erforderlich sind.

sich um die wesentlichen Vertragsbestandteile handelt. In einer anderen Studie zogen es 55 % der befragten Europäer vor, digitale Dienste mit Geld zu bezahlen [Bi16, S. 22]. Zugleich wünscht sich eine Mehrheit ein Verbot von Geschäften mit personenbezogenen Daten [Di14, S. 22]. Ein gesetzliches Verbot müsste einen Ausgleich zwischen den widerstreitenden Grundrechten gewährleisten, *Schulz* in [Go17, § 7 Rn. 24]. Aus dem Recht auf informationelle Selbstbestimmung folgt die staatliche Schutzpflicht, informationellen Selbstschutz für die Nutzer digitaler Dienste tatsächlich zu ermöglichen.[27] Die Möglichkeit, sich vertraglich zur Preisgabe personenbezogener Daten zu verpflichten, könnte mit der Verantwortung des Staates, die Voraussetzungen selbstbestimmter Kommunikationsteilhabe zu gewährleisten, kollidieren, wenn dadurch informationeller Selbstschutz nicht mehr möglich wäre. Auch unter grundsätzlicher Anerkennung der privatrechtlichen Dispositionsfreiheit muss das Recht darauf hinwirken, dass insbesondere bei Vertragspartnern mit überlegenem Verhandlungsgewicht eine einseitige Bestimmungsmacht dieses Vertragspartners nicht die grundrechtlich geschützte Selbstbestimmung in eine Fremdbestimmung verkehrt.[28] Mit Verweis auf ethische Grundsätze wird die rechtliche Anerkennung eines Warenaustauschs von Persönlichkeitsgütern gänzlich abgelehnt [Op17, S. 7].

Selbst bei künftiger Anerkennung einer Gegenleistung in Form einer aktiv-bewussten Dateneingabe als Ausdruck der selbstbestimmten Selbstvermarktung müsste eine interessenausgleichende Regelung mindestens stets gleichwertige Alternativzahlungsmöglichkeiten (in Geld) verpflichtend vorsehen sowie im Umkehrschluss eine Monetarisierung passiv-unbewusst preisgegebener personenbezogener Daten unterbinden. Diese dürften nicht bloß aus dem Anwendungsbereich der Regelung fallen.[29] Selbst im Hintergrund laufende Prozesse, wie das Nutzertracking, könnten vom Nutzer, bspw. durch Betätigen eines Start-Buttons, aktiv angestoßen werden. Andernfalls wäre die vom Richtlinienentwurf anvisierte Gleichstellung entgeltpflichtiger und datengetriebener Geschäftsmodelle nicht erreichbar, wenn eine Umgehung über passiv-unbewusste Datenzugriffe weiterhin möglich und für den Anbieter sogar vorteilhafter, da mit weniger vertragsrechtlichen Pflichten verbunden ist [Op17, S. 12]. Zu beachten wäre zudem, dass Verträge stets unter der auflösenden Bedingung des Widerrufs stünden, da andernfalls ein Eingriff in den Wesensgehalt des Grundrechts zu befürchten ist [AJ17, S. 72]. Da an die vertragsrechtliche Anerkennung „Dienst gegen Daten“ im Hinblick auf Freiwilligkeit und Transparenz sehr hohe Hürden gebunden sind, dürfte nach aktueller Rechtslage keine verbindliche Vereinbarung eines derartigen Geschäftsmodells bestehen. Somit besteht kein Synallagma, das zur Folge hätte, dass App-Anbieter einklagbare Ansprüche auf tatsächliche App-Nutzung und Datenpreisgabe hätten [DK17]. Da Selbstdatenschutzlösungen die passiv-unbewusste Datenpreisgabe adressieren, wird selbst bei Umsetzung des Kommissionsvorschlags der DInhRL-E keine unlautere Verleitung zum Vertragsbruch vorliegen.

[27] BVerfG, stattgebender Kammerbeschluss vom 17. Juli 2013 – 1 BvR 3167/08.
[28] BVerfG, stattgebender Kammerbeschluss vom 23. Oktober 2006 – 1 BvR 2027/02.
[29] Einen Überblick typischer digitaler Geschäftsmodelle, die nicht in den Anwendungsbereich der DinhRL-E fallen würden: [Hä17, S. 737–738].

3.2 Gesamtschau kollidierender Grundrechte

Selbst wenn die Blockade von Datenzugriffen zur Unwirtschaftlichkeit datengetriebener Geschäftsmodelle führen könnte, besteht weder eine gezielte noch eine allgemeine Behinderung.[30] Bei der Gesamtabwägung dürften die Rechte der Anbieter datengetriebener Geschäftsmodelle im Rahmen ihrer Berufsfreiheit[31] hinter den Interessen der Allgemeinheit, Nutzern und Anbietern von Selbstdatenschutzlösungen zurücktreten. Die Grundrechte verkörpern eine objektive Werteordnung, die für alle Bereiche des Rechts gilt.[32] Neben dem Interesse der Nutzer an einem angemessenen Privatsphärenschutz streiten die Berufsfreiheit der Anbieter von Selbstdatenschutzlösungen sowie das Interesse der Allgemeinheit an einer effektiven Rechtsdurchsetzung für deren Zulässigkeit. Anbieter werden mit Geltung der DSGVO Datenminimierung, Privacy by Design und by Default sowie transparente, die Freiwilligkeit sicherstellende Einwilligungsmechanismen umsetzen müssen, sodass bei Nichtbeachtung dieses Defizit ausgeglichen wird. Zu bedenken gilt, dass die technische Durchsetzung gültiger Datenschutzvorgaben einen positiven Wettbewerbsfaktor darstellen kann. Sobald sich sämtliche Wettbewerber gleichermaßen datenschutzkonform verhalten müssen, entsteht ein Level Playing Field zwischen diesen Anbietern. Wettbewerbsvorteile gegenüber datenschutzkonformen Angeboten können dann nicht mehr über unzulässige Datenzugriffe generiert werden.

4 Exkurs: Generierung falscher Daten

In Abschnitt 2.4 wurde bereits auf die mögliche Bereitstellung von Filterfunktionen zur granularen Freigabe oder Blockade von Daten hingewiesen. Anwendungen, die auf fehlende Datensätze mit Fehlfunktionen reagieren, könnten leere oder speziell generierte Ersatzdatensätze geliefert werden. Aus rechtlicher und technischer Sicht ergeben sich hieraus weitere Anforderungen. Das Generieren von falschen Daten wird bereits von einigen Anbietern als Service angeboten. Hierzu zählen bspw. Generatoren, die vollständige Identitäten erzeugen.[33] Auch Selbstdatenschutzanwendungen bieten bereits Lösungen an, die falsche Daten bspw. durch zufälliges Ziehen aus Datenbanken erzeugen. Hier sei exemplarisch die Anwendung „XPrivacy“[34] von Bokhorst genannt. Fraglich ist, ob durch die Bereitstellung von falschen Daten Dritten ein Schaden entstehen könnte, und wie dies im Einzelfall rechtlich zu bewerten ist. Zwar dürfte ein Selbsthilferecht bei datenschutzwidrigen Datenzugriffsversuchen bestehen, die Funktionalitäten könnten aber auch außerhalb datenschutzrechtlich relevanter Konstellationen (bewusst oder unbewusst) eingesetzt werden. Können Nutzer durch gezielte Falscheingabe Vorteile erreichen, könnten sie sich ggf.

[30] Eine allgemeine Marktbehinderung kann vorliegen, wenn die Aktivität zu einer existenziellen Bedrohung für den Mitbewerber führt, vgl. BGH, Urteil vom 24.06.2004 – I ZR 26/02 „*Werbeblocker*“.
[31] Bloße Erwerbschancen sind keine Rechtspositionen im Sinne der Eigentumsgarantie.
[32] BVerfG, Urteil vom 15. Januar 1958 – 1 BvR 400/51 “*Lüth-Urteil*“; LG München, Urteil vom 22.03.2016 – 33 O 5017/15.
[33] Fake Name Generator, ttp://de.fakenamegenerator.com.
[34] https://github.com/M66B/XPrivacy/blob/master/src/biz/bokhorst/xprivacy/PrivacyManager.java.

strafbar machen.[35] Schädigen Falschangaben App-Anbieter, könnte – auch wenn die Datenpreisgabe keine vertragliche Hauptpflicht ist – an eine Nebenpflichtverletzung von Geboten der gegenseitigen Rücksichtnahme zu denken sein (§ 241 Abs. 2 BGB). Daneben sollte ein Missbrauch derartiger Funktionalitäten durch die Nutzer vermieden werden. Der Vertrieb einer Software, die Nutzern die Umgehung vertraglich verbindlich gewordener Spielregeln ermöglicht, wurde als unlauterer Wettbewerb qualifiziert.[36] Zu bedenken gilt auch, dass bei massenhafter Nutzung eine negative Drittwirkung für andere Nutzer nicht ausgeschlossen werden kann.[37] Ein Eingriff in den deliktsrechtlich geschützt eingerichteten und rechtmäßig ausgeübten Gewerbebetrieb kann bei einer gezielten betriebsbezogenen Schädigung vorliegen.[38] Die rechtlichen Auswirkungen bedürfen einer Einzelfallprüfung. Sollen als letzte Eskalationsstufe des Selbstdatenschutzes falsche Daten übermittelt werden, stellen sich mindestens folgende Anforderungen: 1) zufällige Datengenerierung ohne Einflussnahmemöglichkeit der Nutzer, um den missbräuchlichen Einsatz dieser Funktion zu verhindern; 2) Daten müssen plausibel sein, um nicht direkt als Falschdaten entlarvt zu werden; 3) generierte Daten dürfen nicht mit real existierenden Daten identisch sein, um Missbrauch zu unterbinden und keine personenbezogenen Daten Dritter zu verwenden; 4) Einsatz und Auswahl der falschen Daten darf nicht zur rechtswidrigen Schädigung rechtmäßiger Geschäftsmodelle führen. Bei der intelligenten Generierung von Daten können verschiedene Abwägungen getroffen werden. Sehr häufig vorkommende Namenskombinationen (z. B. „Thomas Müller“) erschweren die Identifizierbarkeit. Um zu verhindern, dass weitere Kombinationen, beispielsweise mit Geburtsdaten oder Telefonnummern, zu einer echten Person führen, sollte, sofern die Namen aus einer Datenbank zufällig „gezogen“ werden, die Datenmenge nicht zu klein sein. Folglich muss ein geeigneter Generierungsalgorithmus entwickelt werden. Eine weitere Möglichkeit der Generierung von Ersatzdaten ist das Hinzufügen einer Unschärfe. Dies hat den Vorteil, dass keine Fehlinformationen dargestellt werden. So kann bei Standortdaten der wahre Aufenthaltsort verschleiert und gleichzeitig verhindert werden, dass Anwendungen, die viele Standorte, bspw. zur Generierung von Stauprognosen, abfragen, keine falschen Prognosen berechnen.

5 Fazit und Ausblick

Solange nicht sämtliche Anwendungen Paradigmen wie Privacy by Design und Default berücksichtigen, bietet sich die Verwendung von Selbstdatenschutzanwendungen an. Bis-

[35] Bspw. kann nach KG Berlin, Beschluss vom 22.07.2009 – (4) 1 Ss 181/09 (130/09) bei Anmeldung unter falschem Namen eine Fälschung beweiserheblicher Tatsachen vorliegen (§ 269 StGB), a. A. OLG Hamm, Beschluss vom 18.11.2008 – 5 Ss 347/08. Dies gilt nicht bei sog. Freemium-Angeboten, wenn der Vertragspartner erkennbar kein schutzwürdiges Interesse an der wahren Identität hat.

[36] BGH, Urteil vom 12.01.2017 – I ZR 253/14 „*World of Warcraft II*“.

[37] Bspw. beruhen Geschäftsmodelle wie Stauwarnsysteme auf der Bereitstellung exakter Standortdaten einer Vielzahl von Nutzern.

[38] BGH, Urteil vom 09.12.1958 – VI ZR 199/57 „*Stromunterbrechung*“. Geschützt sind nur rechtmäßige Ausübungsformen eines Betriebs, OLG Karlsruhe, Urteil vom 24.01.1992 – 10 U 163/91.

herige Lösungen werfen jedoch u. a. urheberrechtliche Fragen auf, welche über die Umleitung der Datenkommunikation vermieden werden können. Die Anerkennung von Daten als vertragliche Gegenleistung dürfte lauterkeitsrechtliche Probleme mit sich bringen. Um Widersprüche mit der DSGVO zu vermeiden, sollte die DInhRL-E überarbeitet werden. Große technische Herausforderungen auch im Hinblick auf Privatsphärenschutz durch Generierung falscher Daten ergeben sich aufgrund der heterogenen Umgebung der Anwendersysteme (unterschiedliche Betriebssysteme, Dienste, Geschäftsmodelle und Daten).

Die Veröffentlichung ist im Projekt AVARE („Anwendung zur Verteilung und Auswahl rechtskonformer Datenschutzeinstellungen“) entstanden. Das Projekt wird von der Baden-Württemberg Stiftung gGmbH im Rahmen des Forschungsprogramms „IKT-Sicherheit“ finanziert. Projektträger ist das DLR.

Literaturverzeichnis

[AJ17] Albrecht, Jan Philipp; Jotzo, Florian: Das neue Datenschutzrecht der EU: Grundlagen, Gesetzgebungsverfahren, Synopse, Nomos-Verlag, Baden-Baden, 2017.

[Al16] Alpers, Sascha; Betz, Stefanie; Fritsch, Andreas; Oberweis, Andreas; Pieper, Maria; Schiefer, Gunther; Wagner, Manuela: AVARE Projektbericht, 1. Meilenstein, KIT-Verlag, Karlsruhe, 2016.

[Be17] Europäisches Parlament, Bericht über die Folgen von Massendaten über die Grundrechte, http://www.europarl.europa.eu/

[Bi03] Bishop, Matt: Computer Security: Art and Science. Addison-Wesley Professional, Boston u. a., 2003.

[Bi16] Vodafone Institute for Society and Communication: BIG DATA – a European survey on the opportunities and risks of data analytics, http://www.vodafone-institut.de/bigdata/links/VodafoneInstitute-Survey-BigData-Highlights-en.pdf, 2016.

[Bo13] Bodden, Eric; Rasthofer, Siegfried; Richter, Philipp; Roßnagel, Alexander: Schutzmaßnahmen gegen datenschutzunfreundliche Smartphone-Apps. In: Datenschutz und Datensicherheit 37/11, S. 720–725, 2013.

[Br14a] Brummund, Anke: Smartphones und Apps: Datenschutzrechtliche Risiken und deren Begrenzung. In: (E. Plödereder, L. Grunske, E. Schneider, D. Ull) Informatik 2014, Gesellschaft für Informatik, Bonn, S. 539–550, 2014.

[Br14b] Bräutigam, Peter: Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten. In: MultiMedia und Recht, S. 635–641, 2012.

[Bu10] Buchner, Benedikt: Die Einwilligung im Datenschutzrecht. In: Datenschutz und Datensicherheit 34/1, S. 39–43, 2010.

[Bu17] European Commission: Building a European Data Economy. COM (2017) 9 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN, 2017.

[Da16] Dammann, Ulrich: Erfolge und Defizite der EU-Datenschutzgrundverordnung. Erwar-

teter Fortschritt, Schwächen und überraschende Innovationen, Zeitschrift für Datenschutz, S. 307–314, 2016.

[Di14] Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI): DIVSI Studie Daten – Ware und Währung. Hamburg, Bonn, 2014.

[DK17] Datta, Amit; Klein, Urs Albrecht: Kostenlose Apps – eine vertragsrechtliche Analyse. In: Computer und Recht 33/3, S. 174–181, 2017.

[DS15] Dreier, Thomas; Schulze, Gernot: Urheberrechtsgesetz: Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz: Kommentar, 5. Auflage. München, C.H. Beck, 2015.

[Go17] Gola, Peter (Hrsg.): Datenschutz-Grundverordnung. VO (EU) 2016/679 Kommentar, C.H. Beck, München, 2017.

[Go96] Goldberg, Ian; Wagner, David; Thomas, Randi; Brewer, Eric: A secure environment for untrusted helper applications. In: Proceedings of the 6th conference on USENIX Security Symposium, Focusing on Applications of Cryptography, San José, 1996.

[Hä16] Härting, Niko: Digital Goods und Datenschutz – Daten sparen oder monetarisieren?, In: Computer und Recht 32/11, S. 735–740, 2016.

[HG15] Hornung, Gerrit; Goeble, Thilo: Data Ownership im vernetzten Automobil. In: Computer und Recht 31/4, S. 265–273, 2015.

[Jö16] Jöns, Johanna: Daten als Handelsware. Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI), Hamburg, 2016.

[Kr11] Kremer, Sascha: Vertragsgestaltung bei Entwicklung und Vertrieb von Apps für mobile Endgeräte. In: Computer und Recht 27/12, S. 769–776, 2011.

[Le16] Leistner, Matthias: Die „Metall auf Metall"-Entscheidung des BVerfG. In: Gewerblicher Rechtsschutz und Urheberrecht, S. 772–777, 2016.

[No07] Norberg, Patricia; Horne, Daniel; Horne, David: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. In: Journal of Consumer Affairs 41/1, S. 100–126, 2007

[Op17] European Data Protection Supervisor: Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. https://edps.europa.eu/, 2017.

[Se14] Seidel, Ulrich: Das Grundrecht auf Datensouveränität. In: Zeitschrift für Gesetzgebung, S. 153–165, 2014.

[Sp12] Spindler, Gerald: Grenzen des Softwareschutzes. In: Computer und Recht, 28/7, S. 417–422, 2012.

[Sp17] Specht, Louisa: Konsequenzen der Ökonomisierung informationeller Selbstbestimmung: die zivilrechtliche Erfassung des Datenhandels. Heymanns, Köln, 2012.

[We11] Weigert, Martin: Social Web: Über Konkurrenz und den Nutzen für die User. In: (J. Krone) Medienwandel kompakt 2008–2010, Nomos-Verlag, S. 166–170, 2011.

[Wh14] Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt: White Paper Selbstdatenschutz. 2. Auflage, 2014.