Jonas Botta

ZULÄSSIGKEIT EINER DIGITALEN EINWILLIGUNGSASSISTENZ

Rechtliche Hürden und Lösungsvorschläge für einen nutzerfreundlichen Datenschutz durch Personal Information Management Systems

Vortrag 10 der Reihe „Zu treuen Händen“ | Januar 2022

ZU TREUEN HÄNDEN?
Verbraucherdatenschutz und digitale Selbstbestimmung

Eine Online-Vortragsreihe der Verbraucherzentrale NRW e. V.

mit Unterstützung durch das
Institut für Verbraucherinformatik der Hochschule Bonn-Rhein-Sieg

Impressum

Verbraucherzentrale Nordrhein-Westfalen e.V

Kompetenzzentrum Verbraucherforschung NRW.

Mintropstraße 27

40215 Düsseldorf

zutreuenhaenden@verbraucherzentrale.nrw

Gefördert durch

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

ÜBERARBEITETER NACHDRUCK

Die Erstveröffentlichung des Beitrags erschien als Botta, Jonas. 2021. Delegierte Selbstbestimmung? PIMS als Chance und Risiko für einen effektiven Datenschutz. *Multimedia und Recht* 24, Nr. 12: 946–951.

AUTOR

Dr. Jonas Botta ist Forschungsreferent im Programmbereich „Digitalisierung" am Deutschen Forschungsinstitut für öffentliche Verwaltung und Habilitand an der Deutschen Universität für Verwaltungswissenschaften Speyer.

DOKUMENTION „ZU TREUEN HÄNDEN?“
Alle Videos und Paper der Vortragsreihe finden Sie unter
https://www.verbraucherforschung.nrw/zu-treuen-haenden-tagungsreihe-datenintermediaere-datentreuhaender-60831

INHALT

I. ABSTRACT

Personal Information Management Systems (PIMS) sollen mit ihrer Funktion einer digitalen Einwilligungsassistenz dazu beitragen, dass der Datenschutz im Internet nutzerfreundlicher wird. Um den Verbreitungsgrad dieser Technologie zu erhöhen, hat der Bundesgesetzgeber jüngst die Vorschrift des § 26 TTDSG erlassen. Die datenschutzrechtliche Zulässigkeit einer Einwilligung via PIMS ist jedoch fraglich. Vor diesem Hintergrund untersucht das Working Paper die bestehenden Hürden im geltenden Recht und zeigt Lösungsvorschläge auf.

II. PERSONAL INFORMATION MANAGEMENT SYSTEMS

Wer sich täglich durch unzählige Cookie- bzw. Consent-Banner klicken muss, um online Zeitung zu lesen oder Überweisungen zu tätigen, dem wird es in der Regel schwerfallen, das Erfordernis seiner datenschutzrechtlichen Einwilligung nicht als bloße Last, sondern als Ausdruck seiner persönlichen Entscheidungsfreiheit zu begreifen. Um diesen Widerspruch zwischen normativer und tatsächlicher Bedeutung der Einwilligung aufzulösen, wird seit einigen Jahren der Einsatz von Personal Information Management Systems (PIMS) diskutiert. Hierbei handelt es sich um eine sogenannte Privacy-enhancing Technology (PET), das heißt um eine datenschutzfördernde Technologie (Janssen et al. 2020, 7 ff.). Die Befürworter der PIMS – namentlich etwa die EU-Kommission oder die deutsche Bundesregierung – erhoffen sich von ihnen eine Neuausrichtung der Datenwirtschaft: Die bisherige Anbieterzentrierung soll einer verstärkten Nutzerzentrierung weichen.

Der EU-Datenschutzbeauftragte definiert PIMS als Systeme, die personenbezogene Daten in sicheren, lokalen oder Online-Speichern verwalten und dem Einzelnen die Kontrolle über die Weitergabe der ihn betreffenden personenbezogenen Daten bieten (Europäischer Datenschutzbeauftragter 2016, 226). Dafür sollen PIMS zukünftig insbesondere als Einwilligungsmanagementsysteme fungieren. Sie sollen dem Einzelnen sowohl einen Überblick über die von ihm erklärten Einwilligungen verschaffen als auch ihn bei der Einwilligungserklärung selbst unterstützen. Letzteres soll die Auswahl abstrakt-genereller Datenschutzpräferenzen im PIMS ermöglichen, auf deren Grundlage das Assistenzsystem eine Einwilligung im konkret-individuellen Fall automatisiert erklären kann. Das Dauerklicken durch den Cookie-Banner-Dschungel könnte damit sein Ende finden. Zur Erreichung dieses Ziels sind jedoch nicht nur technische, sondern auch rechtliche Hürden zu nehmen.

III. RECHTLICHER RAHMEN EINER DIGITALEN EINWILLIGUNGSASSISTENZ

Wie es datenschutzrechtlich zu bewerten ist, wenn Nutzer via PIMS automatisiert in die Platzierung und den Abruf von Cookies einwilligen können, richtet sich zuvorderst nach der europäischen Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-RL)[1]

[1] Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-RL) (2002/58/EG bzw. 2009/136/EG) http://data.europa.eu/eli/dir/2002/58/2009-12-19.

beziehungsweise ihrem Art. 5 Abs. 3 S. 1. Danach setzen die Speicherung von Informationen sowie der Zugriff auf Informationen auf Endgeräten grundsätzlich eine Einwilligung voraus. Als Richtlinie entfaltet die ePrivacy-RL indes keine unmittelbare Wirkung. Vielmehr verpflichtet sie die EU-Mitgliedstaaten, ihre Vorschriften in eigenes Recht umzusetzen (vgl. Art. 288 Abs. 3 AEUV).

1. TELEKOMMUNIKATION-TELEMEDIEN-DATENSCHUTZGESETZ

Der Bundesgesetzgeber hat Art. 5 Abs. 3 S. 1 ePrivacy-RL mit § 25 Abs. 1 S. 1 Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)[2] in nationales Recht umgesetzt. Im Unterschied zur ePrivacy-RL sieht das am 01.12.2021 in Kraft getretene TTDSG darüber hinaus eine spezielle Regelung für PIMS vor (Piltz 2021, 563). Konkret können sich sogenannte Dienste zur Verwaltung von nach § 25 TTDSG erteilten Einwilligungen um eine staatliche Anerkennung bemühen. Eine generelle Anerkennungspflicht für PIMS-Anbieter besteht gemäß dem Wortlaut der Norm allerdings nicht. § 26 TTDSG soll ihnen gemäß der Gesetzesbegründung einen sicheren und ermöglichenden Rechtsrahmen bieten.[3]

Anerkennungsvoraussetzungen sind unter anderem, dass die Dienste kein wirtschaftliches Eigeninteresse verfolgen und ihre Datenverarbeitung auf Zwecke der Einwilligungsverwaltung beschränkt bleibt (§ 26 Abs. 1 Nr. 2 und Nr. 3 TTDSG). Der Bundesgesetzgeber hat sich damit gegen die Überlegung entschieden, dass Nutzer ihre Daten via PIMS monetarisieren können. Dennoch ist auch ein kommerzielles PIMS-Angebot nicht generell ausgeschlossen, da sich das Verbot wirtschaftlicher Eigeninteressen auf die Datenverwertung und nicht auf die Einwilligungsverwaltung als solche bezieht (Dürschmied 2021, 396). Um die Anerkennungsvoraussetzungen näher auszugestalten, ist der Erlass einer Rechtsverordnung vorgesehen (§ 26 Abs. 2 TTDSG).

Zur digitalen Einwilligungsassistenz selbst schweigt sich § 26 TTDSG aus. In § 26 Abs. 1 Nr. 1 TTDSG hat der Bundesgesetzgeber lediglich klargestellt, dass die Norm für Dienste gilt, die die Einholung und Verwaltung von Einwilligungen ermöglichen. Unter welchen Bedingungen eine automatisierte Einwilligungserklärung zulässig ist, beantwortet das Gesetz aber nicht. In seiner Begründung heißt es nur, dass die Dienste zur Einwilligungsverwaltung schon „nach jetziger Rechtslage möglich“ seien.[4] Ob diese Rechtsauffassung überzeugt, hängt von der Datenschutzgrundverordnung (DSGVO)[5] ab, auf die auch § 25 Abs. 1 S. 2 TTDSG verweist. Im Gegensatz zur ePrivacy-RL ist die DSGVO unmittelbar anwendbares Unionsrecht (vgl. Art. 288 Abs. 2 AEUV).

2. DATENSCHUTZ-GRUNDVERORDNUNG

In der DSGVO hat der Unionsgesetzgeber neben den Einwilligungsvoraussetzungen auch das Konzept „Datenschutz durch Technik“ verankert. Nach Art. 25 DSGVO müssen bereits bei der Entwicklung und nicht erst bei der Anwendung neuer Technologien datenschutzrechtliche Vorgaben Beachtung finden und durch technische sowie organisatorische Maßnahmen abgesichert werden (Eichenhofer 2021, 396). Für Technologien, die nicht nur datenschutzkonform zum Einsatz kommen, sondern selbst Datenschutz fördern sollen, fehlt es hingegen an einer gesonderten Regelung. Die DSGVO

---

[2] Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) (BGBl. 2021 I S. 1982).

[3] Deutscher Bundestag, Drucksache 19/29839 vom 19.05.2021.

[4] Deutscher Bundestag, Drucksache 19/29839 vom 19.05.2021.

[5] Datenschutz-Grundverordnung (DSGVO) (2016/679) https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679.

beinhaltet aufgrund ihres „One size fits all“-Ansatzes insbesondere keine Privilegierungen für PET. Sollen PIMS als digitale Einwilligungsassistenten zum Einsatz kommen, sind die Einwilligungsvoraussetzungen der Art. 4 Nr. 11, Art. 6 Abs. 1 Unterabs. 1 lit. a und Art. 7 DSGVO vollumfänglich zu beachten.

2.1 Erklärungsakt

Eine wirksame Einwilligung setzt zunächst einen Erklärungsakt voraus.

(1) Wer erklärt die Einwilligung?

Willigt ein PIMS für den Nutzer in das Webtracking ein, lässt sich diese Erklärung entweder als unmittelbare Einwilligung des Nutzers oder als (eigene oder fremde) Erklärung des Systems ansehen. Maßgeblich ist hierbei der Grad an technischer Autonomie, der dem Assistenzsystem bei der Einwilligungserklärung zukommt (Specht-Riemenschneider 2019, 45–48). Ein PIMS benötigt einen umso größeren Entscheidungsspielraum, je abstrakter die vom Nutzer ausgewählten Datenschutzpräferenzen gefasst sind und je komplexer das Webtracking ist. Teilweise wollen Websites über 300 Cookies platzieren, insbesondere auch sogenannte Third Party Cookies (Cahn et al. 2016, 900).

Lässt sich die Einwilligung via PIMS auf die automatisierte Übermittlung der Datenschutzpräferenzen nach einem „Wenn-dann-Schema“ beschränken, ist eine unmittelbare Einwilligungserklärung des Nutzers zu bejahen. Eine derartige Erklärung mittels Auswahl technischer Einstellungen ist nach ErwGr. 32 S. 2 DSGVO zulässig. Sollen PIMS jedoch nicht nur Nutzereingaben eins zu eins umsetzen, sondern aufgrund der abstrakt-generellen Datenschutzpräferenzen auch komplexere Einwilligungsanfragen bewerten und beantworten können, setzt dies eine gewisse Autonomie voraus. Entscheidend ist dann, inwieweit dem Nutzer die Erklärung des PIMS gegenüber dem jeweiligen Einwilligungsempfänger zurechenbar ist.

(2) Zulässigkeit einer Vertretungsmöglichkeit

In der DSGVO findet sich keine ausdrückliche Regelung zur Vertretungsmöglichkeit bei der Einwilligungserklärung. Auf den ersten Blick wäre es daher erwägenswert, wie schon unter der Geltung des BDSG a. F., auf die Rechtsfiguren der Botenschaft und Stellvertretung zurückzugreifen. Ein unmittelbarer Rückgriff auf das nationale Zivilrecht – insbesondere die §§ 164 ff. BGB (analog) – für die Frage nach dem „Ob“ der Vertretungsmöglichkeit scheidet jedoch aus. Die DSGVO ist grundsätzlich unionsautonom auszulegen. Allein im Rahmen der sogenannten Öffnungsklauseln ist mitgliedstaatliches Recht zu berücksichtigen, insoweit die nationalen Gesetzgeber von ihrer Regelungsbefugnis Gebrauch gemacht haben. Für den Erklärungsakt der Einwilligung existiert jedoch keine Öffnungsklausel (Specht-Riemenschneider 2019, 41).

Der Wortlaut der Einwilligungsdefinition in Art. 4 Nr. 11 DSGVO spricht gegen eine Vertretungsmöglichkeit. Dort ist von der Einwilligung „der betroffenen Person“ die Rede. Daraus ließe sich ableiten, dass es sich bei der Einwilligungserklärung um einen höchstpersönlichen Akt handelt, der keiner Vertretung zugänglich ist (Klement 2019, 37). Eine derartige Sichtweise findet zudem eine argumentative Stütze in der grundrechtlichen Verankerung der Einwilligung in Art. 8 Abs. 2 S. 1 GRCh.[6]

[6] Charta der Grundrechte der Europäischen Union, Art. 8 Schutz personenbezogener Daten https://eur-lex.europa.eu/eli/treaty/char_2012/oj.

Aus Art. 8 Abs. 1 S. 2 DSGVO ergibt sich indes, dass vor der Vollendung des 16. Lebensjahrs eine Einwilligung durch die Träger der elterlichen Verantwortung erteilt werden kann. Daraus ist zu folgern, dass der Unionsgesetzgeber bei der Regelung der Einwilligungsvoraussetzungen nicht von ihrer Höchstpersönlichkeit ausgegangen ist. Anderenfalls hätte er den Minderjährigenschutz auch durch ein generelles Einwilligungsverbot ausgestalten können. Unterstützend lässt sich zudem anführen, dass sich auch an anderer Stelle in der DSGVO eine Vertretungsregelung findet. Art. 80 DSGVO statuiert, dass sich Betroffene bei der Geltendmachung ihrer Rechte aus den Artikeln 77, 78, 79 und 82 DSGVO vertreten lassen können. Im Ergebnis ist eine Einwilligungserklärung via PIMS dem Nutzer zurechenbar.

(3) Wirksame Bevollmächtigung des PIMS

Um die strengen Voraussetzungen an eine wirksame Einwilligung nicht zu unterlaufen, sind an die Bevollmächtigung des PIMS als Vertreter seines Nutzers dieselben Anforderungen wie an die Einwilligung selbst zu stellen (Buchner und Kühling 2020, 31). Dabei ist allein das Verhältnis zwischen Nutzer und PIMS maßgeblich, während die Wirksamkeit der Einwilligung auch von ihrem Empfänger abhängt.

Insbesondere gilt es kritisch zu beleuchten, ob die Bevollmächtigung freiwillig erteilt worden ist (Datenethikkommission 2019, 133). An der Freiwilligkeit kann es fehlen, wenn zwischen dem Nutzer und dem Anbieter des PIMS ein Machtungleichgewicht besteht (vgl. ErwGr. 43 S. 1 DSGVO). Ein solches Machtungleichgewicht wäre anzunehmen, wenn der PIMS-Anbieter eine Monopolstellung innehätte, das heißt, wenn der digitale Raum nicht mehr ohne die Nutzung seines Dienstes betretbar wäre. Derartige Entwicklungen lässt der Siegeszug von „Single Sign-on“-Verfahren bei den Big Tech befürchten (Schwartmann et al. 2020, 231). Dass auch die PIMS-Anbieter zu Gatekeepern werden könnten, ist derzeit jedoch unwahrscheinlich.

2.2 Bestimmtheit

Die Einwilligungserklärung muss des Weiteren für einen bestimmten Fall erfolgen, das heißt, es muss feststehen, in welche Datenverarbeitung der Betroffene konkret einwilligt (Klement 2019, 68). Insbesondere darf der Verarbeitungszweck nicht zu pauschal gefasst sein. Eine generelle Einwilligung ins Webtracking ist unzulässig (Buchner und Kühling 2020, 62). Zwar lässt sich grundsätzlich vertreten, dass an die Einwilligung via PIMS niedrigere Konkretisierungsanforderungen anzulegen sind, insoweit sie dem Datenschutz förderlich ist (Kühling 2021, 10). Entscheidend sind aber stets das jeweilige Abstraktionsniveau der Datenschutzpräferenzen und die Komplexität der Datenverarbeitung. Lässt sich zu dem Zeitpunkt, indem der Nutzer seine Präferenzen ins PIMS einträgt, noch nicht ausreichend abbilden, in welches individuell-konkrete Webtracking das System später einwilligen soll, kann dem Bestimmtheitserfordernis nicht entsprochen werden (Klement 2019, 71). Damit scheidet insbesondere der Einsatz lernfähiger PIMS aus. Sie könnten Einwilligungserklärungen nur vorbereiten. Der praktische Vorteil der PIMS, die einmalige Eingabe von Datenschutzpräferenzen anstelle des Dauerklickens durch den Cookie-Banner-Dschungel, mutiert zu ihrem rechtlichen Nachteil, wenn die Systeme nicht deterministisch sind.

2.3 Informiertheit

Die konkreten Umstände einer jeden Datenverarbeitung müssen zudem nicht nur objektiv bestimmt sein, die betroffene Person muss von ihnen auch subjektiv Kenntnis er-

langt haben (Klement 2019, 72). Auch dieses Informationserfordernis schränkt die Anwendungsmöglichkeit von PIMS erheblich ein. Denn der Nutzer muss zeitlich vor der Datenverarbeitung derart über diese informiert worden sein, dass er sich eine Vorstellung von den Folgen seiner Einwilligung verschaffen kann (Buchner und Kühling 2020, 59). Es stellt aber eine erhebliche Herausforderung dar, im Zeitpunkt der Präferenzeingabe über sämtliche nachfolgenden Tracking- und Datenverarbeitungsvorgänge verständlich zu informieren (Sesing 2021, 548). Der dabei benötigte Detailgrad steht potenziell im Widerspruch zu dem abstrakt-generellen Ansatz der digitalen Einwilligungsassistenz. Ein erhebliches Informationsdefizit folgt zudem auch daraus, dass PIMS-Anbieter und Einwilligungsempfänger personenverschieden sind. Allein Letztere haben es in der Hand, dem Assistenzsystem die notwendigen Informationen, wie etwa ihre Identität (ErwGr. 42 S. 4 DSGVO), zur Verfügung zu stellen.

3. ePRIVACY-VERORDNUNG

Der Rechtsrahmen für PIMS beschränkt sich nicht auf das TTDSG und die DSGVO. Perspektivisch soll die ePrivacy-Verordnung die ePrivacy-RL ersetzen. In der Folge ersetzte sie aufgrund ihres Anwendungsvorrangs indirekt auch das TTDSG, soweit dieses auf der ePrivacy-RL basiert. Ursprünglich hätte die ePrivacy-Verordnung schon zeitgleich mit der DSGVO Geltung erlangen sollen (vgl. Art. 27 Abs. 1 des Kommissionsentwurfs).[7] Doch die Trilog-Verhandlungen haben erst 2021 begonnen. Damit ist noch offen, ob und inwieweit die Vorgaben der zukünftigen Verordnung über die jetzigen Regelungen der Richtlinie beziehungsweise des TTDSG hinausgehen werden. Die EU-Kommission hat in ihrem Verordnungsentwurf jedenfalls am Einwilligungserfordernis festgehalten (Art. 8 Abs. 1 lit. b) und zugleich eine Regelung zur Einwilligung durch Browsereinstellungen vorgesehen (Art. 9 Abs. 2). Auch der Rat der EU hat sich in seinem Verhandlungsmandat dafür ausgesprochen, Einwilligungen durch technische Einstellungen zuzulassen (Art. 4a Nr. 2).[8] Es ist daher denkbar, dass Deutschland sich unter Bezugnahme auf das TTDSG nun auf Unionsebene für eine konkrete PIMS-Regelung einsetzen wird.

4. DATA GOVERNANCE ACT

Der Data Governance Act, der einen einheitlichen Rechtsrahmen für die sektorspezifischen gemeinsamen europäischen Datenräume schaffen soll (ErwGr. 2 DGA)[9], tritt 2022 in Kraft. Auch er wird für PIMS relevant werden. Die Art. 9 ff. DGA enthalten Regelungen für sogenannte Datenintermediäre. Darunter fallen insbesondere Vermittlungsdienste zwischen Betroffenen, die ihre Daten zugänglich machen wollen und potenziellen Datennutzern (Art. 9 Abs. 1 lit. b DGA). PIMS werden sich zumindest teilweise hierunter subsumieren lassen. Dann bedarf es für ihren Einsatz einer behördlichen Anmeldung (Art. 10 DGA) und der Einhaltung spezieller Bedingungen (Art. 11

[7] Europäische Kommission, Vorschlag für Verordnung über Privatsphäre und elektronische Kommunikation COM (2017) final vom 10.01.2017
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52017PC0010.

[8] Council of the European Union, Proposal for a Regulation on Privacy and Electronic Communications – Mandate for negotiations with EP 6087/21 final vom 10.02.2021
https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[9] Europäische Kommission, Vorschlag für eine Verordnung über europäische Daten-Gorvernance COM (2020) 767 final vom 25.11.2020
https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:52020PC0767.

DGA). Dadurch wird sich der Erfüllungsaufwand für PIMS-Anbieter potenziell weiter erhöhen, da die Vorgaben nicht deckungsgleich mit denen des § 26 TTDSG sind.

5. BEWERTUNG DES RECHTLICHEN RAHMENS UND VORSCHLÄGE ZU SEINER FORTENTWICKLUNG

Der Plan des Bundesgesetzgebers, die Verbreitung von PIMS durch einen speziellen Rechtsrahmen zu fördern, dürfte nicht wie gewünscht aufgehen. Zu sehr schränkt die DSGVO die Einsatzmöglichkeiten der PIMS als digitale Einwilligungsassistenten ein. Entscheidend für ihren Erfolg ist, ob sich eine abstrakt-generelle Einwilligungserklärung doch noch auf ein rechtlich tragendes Fundament stellen lässt. Darüber hat jedoch nicht der Bundes-, sondern der Unionsgesetzgeber zu entscheiden (Hanloser 2021, 402). Letzterer hat es bislang versäumt, PET besonders zu fördern.

5.1 Erster Vorschlag: Experimentierklausel für Privacy-enhancing Technologies

Um zukünftig die Entwicklung und den Einsatz datenschutzfördernder Technologien zu erleichtern, sollte der Unionsgesetzgeber das Datenschutzrecht um eine Experimentierklausel für PET ergänzen. Sie könnte die Möglichkeit eröffnen, bei der zuständigen Datenschutz-Aufsichtsbehörde zeitlich befristete Ausnahmen von den Vorschriften des Datenschutzrechts zu beantragen. So ließen sich die Potenziale einer digitalen Einwilligungsassistenz rechtssicher erproben. Eine derartige „regulatorische Sandkiste“ wäre auch vorzugswürdig gegenüber der Alternative, die Einwilligungsvoraussetzungen allgemein und damit das Datenschutzniveau insgesamt abzusenken. Eine Experimentierklausel hätte darüber hinaus den Vorteil, dass sie nicht auf eine bestimmte Technologie begrenzt sein müsste, sondern auch offen für weitere sein kann. Um die tatsächliche Wirkung der Klausel überprüfen zu können, sollte in ihr ein Evaluationsmechanismus verankert sein. Auf der Grundlage der dadurch erlangten Erkenntnisse könnte das Datenschutzrecht dauerhaft für PET spezifisch angepasst werden.

Da der Rat der EU die Schaffung von Experimentierklauseln ausdrücklich befürwortet, besteht die Chance, dass dieser Vorschlag Wirklichkeit werden könnte.[10] Das Konzept der „regulatorischen Sandkiste“ ist den Datenschutz-Aufsichtsbehörden zudem nicht unbekannt. Das britische Information Commissioner's Office hat bereits 2019 ein spezielles Beratungsprogramm für die Entwicklung neuer Technologien gestartet. Auch der Kommissionsentwurf einer KI-Verordnung sieht Reallabore für innovative KI-Systeme vor, an denen die Datenschutz-Aufsichtsbehörden beteiligt sein sollen (Art. 53 ff.).[11] Neu wäre indes eine Schonfrist von den gesetzlichen Vorgaben.

5.2 Zweiter Vorschlag: Kooperationspflichten für Browser- und Telemedienanbieter verschärfen

Der Erfolg der PIMS hängt zudem davon ab, inwieweit Browser- und Telemedienanbieter ihre Nutzung anerkennen und durch Schnittstellen ermöglichen. Fehlt es hieran, könnten sie das Schicksal des Platform for Privacy Preferences Project (P3P) teilen,

[10] Rat der Europäischen Union, Schlussfolgerungen zu Reallaboren und Experimentierklauseln 12683/20 final vom 16.11.2020 https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/de/pdf.

[11] Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz COM (2021) 206 final vom 21.04.2021 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:52021PC0206.

das bereits vor 20 Jahren Datenschutzinformationen nutzerfreundlich vermitteln wollte, sich in der Praxis aber nie durchsetzen konnte.

Während Browseranbieter nach geltendem Recht die Einbindung von PIMS zu berücksichtigen und die im System gespeicherten Datenschutzeinstellungen sogar zu befolgen haben (§ 26 Abs. 2 Nr. 3 lit. a) TTDSG), müssen Telemedienanbieter wie Websitebetreiber die Einbindung und Einstellungen von PIMS insgesamt nur berücksichtigen (§ 26 Abs. 2 Nr. 3 lit. b) TTDSG). Allein schon aufgrund der bestehenden Rechtsunsicherheiten ist daher anzunehmen, dass zahlreiche Telemedienanbieter weiterhin (zusätzlich) eine unmittelbare Einwilligung der Internetnutzer verlangen werden (Dürschmied 2021, 226). Dass Telemedienanbieter die PIMS-Nutzung ignorieren, ist insbesondere zu befürchten, wenn das System die Einwilligung verweigert hat. Sie könnten dann umso mehr versucht sein, via Consent-Banner doch noch eine Einwilligung zu erlangen.

Der Bundesgesetzgeber sollte vor diesem Hintergrund sowohl für Browser- als auch für Telemedienanbieter eine umfassende Kooperationspflicht mit anerkannten PIMS begründen und diese in der Rechtsverordnung nach § 26 Abs. 2 TTDSG näher ausgestalten (Datenethikkommission 2019, 134). Damit wäre zugleich ein erheblicher Anreiz für PIMS-Anbieter gesetzt, sich staatlich anerkennen zu lassen. Dies hätte zur Folge, dass ihr Geschäftsmodell nicht allein aus der Datenkommerzialisierung bestehen darf (zum Verbot wirtschaftlicher Eigeninteressen siehe III. 1.).

IV. RISIKEN DES PRIVACY SELF-MANAGEMENT

Die Förderung von PIMS als digitale Einwilligungsassistenten ist Ausdruck eines Regulierungsansatzes im Datenschutzrecht, der auch als Privacy Self-Management bezeichnet wird (Solove 2013, 1880). Dieser individualistische Ansatz stellt die Einwilligung in den Mittelpunkt, da sie im System der datenschutzrechtlichen Erlaubnistatbestände der betroffenen Person den meisten Einfluss auf die Datenverarbeitung garantiert. Die Zustimmung zur Datenverarbeitung unterliegt ihrer Entscheidungsfreiheit und kann jederzeit widerrufen werden (Art. 7 Abs. 3 DSGVO).

Zugleich kann eine Einwilligung aber weitergehendere Verarbeitungsrechte als die gesetzlichen Rechtsgrundlagen legitimieren, da sie nicht im selben Maße dem Erforderlichkeitsgebot unterliegt (vgl. § 25 Abs. 2 Nr. 2 TTDSG). Das kann Verantwortliche dazu verleiten, möglichst viele Verarbeitungsvorgänge auf die Einwilligung zu stützen. Dass sich die betroffene Person demgegenüber behaupten kann, sollen die umfassenden Informationspflichten sicherstellen. Die Komplexität der ubiquitären Datenverarbeitung, ihrer Zwecke und Akteure nimmt indes immer weiter zu. Ein Phänomen, das sich beim Einsatz von PIMS noch verschärft, da diese den Nutzer umfassend über eine Vielzahl von Verarbeitungsvorgängen und Trackingmechanismen in Kenntnis setzen müssen (Sesing 2021, 548).

Selbst wenn PIMS ihren Nutzern die notwendigen Informationen vermitteln können, hängt es stets vom Einzelnen ab, ob er sich tatsächlich ein umfassendes Bild von der Datenverarbeitung verschaffen will. Zudem kann auch ein datenschutzsensibler PIMS-Nutzer nicht mit absoluter Gewissheit prognostizieren, welche Konsequenzen seine Einwilligung haben wird, wenn weitere Akteure (durch Third Party Cookies) involviert sind. Eine zu starke Einwilligungsfokussierung birgt daher die Gefahr, bestehende

Machtungleichgewichte im digitalen Raum nicht zu überwinden, sondern zu verfestigen, da sich hierdurch die Grundbedingungen der Datenwirtschaft nicht verändern (Janssen et al. 2020, 13–18).

Eine vorrangig einwilligungsbasierte Regulierung blendet zudem aus, dass personenbezogene Daten nicht stets nur einem Individuum zuordenbar sind. Oftmals sind sie – abhängig vom jeweiligen Verarbeitungskontext – auch drittbezogen (Schantz 2019, 7). Willigt aber nur eine Person in die Verarbeitung dieser Daten ein, können die Rechte der anderen betroffenen Personen verletzt werden.

Setzt der Gesetzgeber verstärkt auf Privacy Self-Management, erfolgen daraus somit nicht nur Chancen für einen nutzerzentrierten Datenschutz, sondern auch Risiken für ein gleichwertiges und hohes Datenschutzniveau. Zumindest wenn er es unterlässt, die Datenwirtschaft auch selbst durch verbindliche Vorgaben zu regulieren. Ein derartiger Regelungsrahmen für die Zulässigkeit von Webtracking fehlt aber bislang (Wenhold 2018, 263–265). Die Förderung der PIMS sollte vor diesem Hintergrund Teil eines umfassenden Regulierungskonzepts sein.

V. FAZIT

PIMS versprechen als digitale Einwilligungsassistenten einen Ausweg aus dem Cookie-Banner-Dschungel. Ist der Internetnutzer in die Lage versetzt, seine Datenschutzpräferenzen nur noch abstrakt-generell festzulegen, statt bei jedem Onlineangebot neu entscheiden zu müssen, kann das grundsätzlich zu bewussteren Entscheidungen führen. Bislang steckt die Entwicklung dieser Technologie aber noch in ihren Anfängen.

Ob § 26 TTDSG dies zeitnah ändern wird, ist angesichts der bestehenden Rechtsunsicherheiten unwahrscheinlich. Der Bundesgesetzgeber kann sich insbesondere nicht über die Einwilligungsvoraussetzungen der DSGVO hinwegsetzen. Für die Verbreitung von PIMS kommt es somit auf die Fortentwicklung des unionalen Datenschutzrechts an. Eine Experimentierklausel für PET könnte wegweisend sein, um zukünftig Datenschutz durch Recht und durch Technik besser zu verzahnen. Außerdem sollten Browser- und Telemedienanbieter noch stärker in die Pflicht genommen werden, mit PIMS zu kooperieren. Ansonsten wird ihr Erfolg an fehlenden Schnittstellen und doppelten Einwilligungsersuchen scheitern.

Nutzerfreundliche Technologien sind unterdessen kein Allheilmittel, um den Machtasymmetrien in der Datenwirtschaft entgegenzuwirken. Überlässt es der Gesetzgeber nur dem Einzelnen, seine Rechte durchzusetzen, stiehlt er sich aus seiner grundrechtlichen Verantwortung, die informationelle Selbstbestimmung zu schützen. Gerade für das Webtracking durch Cookies & Co. sollte zukünftig weniger auf ein Einwilligungserfordernis als vielmehr auf klare gesetzliche Regelungen gesetzt werden. Die Gelegenheit hierfür bietet die neue ePrivacy-Verordnung.

VI. HANDLUNGSEMPFEHLUNGEN

1. Der Unionsgesetzgeber sollte eine Experimentierklausel im Datenschutzrecht verankern, um die Entwicklung und den Einsatz von Privacy-enhancing Technologies wie PIMS zu fördern.

2. Im Rahmen der neuen ePrivacy-Verordnung sollte der Unionsgesetzgeber klare gesetzliche Vorgaben für die Zulässigkeit von Webtracking formulieren, statt weiterhin vorrangig auf den Erlaubnistatbestand der Einwilligung zu setzen.

3. Der Bundesgesetzgeber sollte die Kooperationspflichten für Browser- und Telemedienanbieter mit PIMS verschärfen, damit für diese ein Anreiz besteht, sich nach § 26 TTDSG anerkennen zu lassen und die darin verankerten Vorgaben wie das Verbot wirtschaftlicher Eigeninteressen einzuhalten.

4. Der Bundesgesetzgeber sollte prüfen, ob die deutsche PIMS-Regulierung über die ePrivacy-Verordnung hinaus gelten soll (und kann).

VII. LITERATURVERZEICHNIS

Buchner, Benedikt, und Jürgen Kühling. 2020. Artikel 7. In: *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar*, hg. von Jürgen Kühling und Benedikt Buchner. 3. Auflage. München: C.H. Beck.

Cahn, Aaron, Scott Alfeld, Paul Barford und S. Muthukrishnan. 2016. An Empirical Study of Web Cookies. In: *Proceedings of the 25th International Conference on World Wide Web*, 891–901. https://doi.org/10.1145/2872427.2882991.

Dürschmied, Christian. 2021. Ausnahmen von der Einwilligungspflicht und Personal-Information-Management-Systeme im TTDSG. *Datenschutz-Berater* 7–8, Nr. 21: 224–226.

Datenethikkommission. 2019. *Gutachten der Datenethikkommission*. Berlin. https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 (Zugriff: 21.12.2021).

Eichenhofer, Johannes. 2021. *e-Privacy: Theorie und Dogmatik eines europäischen Privatheitsschutzes im Internet-Zeitalter*. Tübingen: Mohr Siebeck.

Europäischer Datenschutzbeauftragter. 2016. *Stellungnahme 9/2016 zu Systemen für das Personal Information Management (PIM)*. Brüssel.

Hanloser, Stefan. 2021. Schutz der Geräteintegrität durch § TTDSG § 25 TTDSG: Neue Cookie-Regeln ab dem 1.12.2021. *Zeitschrift für Datenschutz*: 399–403.

Information Commissioner's Office. o. D. *The Guide to the Sandbox*. https://ico.org.uk/for-organisations/regulatory-sandbox/the-guide-to-the-sandbox/ (Zugriff: 21.12.2021).

Janssen, Heleen, Jennifer Cobbe und Jatinder Singh. 2020. Personal information management systems: a user-centric privacy utopia? *Internet Policy Review* 9, Nr. 4. https://doi.org/10.14763/2020.4.1536.

Klement, Jan Henrik. 2019. Artikel 7. In*: Datenschutzrecht, DSGVO mit BDSG, Kommentar*, hg. von Spiros Simitis, Gerrit Hornung und Indra Spiecker gen. Döhmann. Baden-Baden: Nomos.

Kühling, Jürgen. 2021. Der datenschutzrechtliche Rahmen für Datentreuhänder: Chance für mehr Kommerzialisierungsfairness und Datensouveränität? *Zeitschrift für Digitalisierung und Recht*: 1–26.

Piltz, Carlo. 2021. Das neue TTDSG aus Sicht der Telemedien: Anwendungsbereich, Tracking und Aufsichtsbehörden. *Computer und Recht* 37, Nr. 8: 555–565.

Schantz, Peter. 2019. Artikel 6 Abs. 1. In: *Datenschutzrecht, DSGVO mit BDSG, Kommentar*, hg. von Spiros Simitis, Gerrit Hornung und Indra Spiecker gen. Döhmann. Baden-Baden: Nomos.

Schwartmann, Rolf, Kristin Benedikt, und Yvette Reif. 2020. Datenschutz bei Websites – aktuelle Rechtslage und Ausblick auf das TTDSG. *Recht der Datenverarbeitung* 5: 231–236.

Sesing, Andreas. 2021. Cookie-Banner – Hilfe, das Internet ist kaputt! Ansätze zur Verbesserung der Nutzererfahrung. *Multimedia und Recht* 24: 544–549.

Solove, Daniel J. 2013. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 126, Nr. 7: 1880–1903.

Specht-Riemenschneider, Louisa. 2019. *Diktat der Technik: Regulierungskonzepte technischer Vertragsinhaltsgestaltung am Beispiel von Bürgerlichem Recht und Urheberrecht*. Baden-Baden: Nomos.

Spindler, Gerald. 2021. Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E) – Ansatz, Instrumente, Qualität und Kontext. *Computer und Recht* 37, Nr. 6: 361–374.

Wenhold, Céline. 2018. *Nutzerprofilbildung durch Webtracking: Zugleich eine Untersuchung zu den Defiziten des Datenschutzrechts im Zeitalter von Big Data-Anwendungen*. Baden-Baden: Nomos.