Deutscher Bundestag

Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)106

verbraucherzentrale
Bundesverband

20 JAHRE
gemeinsam
wirksam

RECHTE DER VERBRAUCHER IN DER DATENGETRIEBENEN GESELLSCHAFT STÄRKEN

Stellungnahme des Verbraucherzentrale Bundesverbands im Rahmen der Anhörung des Ausschusses Digitale Agenda des Deutschen Bundestags zur Datenstrategie der Bundesregierung

22. Februar 2021

Impressum

Verbraucherzentrale
Bundesverband e.V.

Team
Digitales und Medien

Rudi-Dutschke-Straße 17
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

INHALT

I. ZUSAMMENFASSUNG 3

II. EINLEITUNG 5

III. POSITIONEN IM EINZELNEN 6

1. Allgemein ... 6
    1.1 Ziele und Ausrichtung der Datenstrategie ... 6
    1.2 „Verantwortungsvolle“ und „innovative“ Datennutzung ... 6
2. Dateninfrastruktur ... 7
3. Datennutzung ... 7
    3.1 Regelungsbedarf im Datenschutzrecht ... 7
    3.2 Anonymisierung ... 8
    3.3 Datenintermediäre ... 10
    3.4 Datenschutz durch Technikgestaltung ... 11
    3.5 Datenübertragbarkeit ... 12
    3.6 Datenschutzaufsicht ... 13
    3.7 Algorithmenbasierte Entscheidungssysteme ... 14
    3.8 IT-Sicherheit ... 15
    3.9 Weitere Stärkung der Verbraucherrechte in der Datenökonomie ... 16
    3.10 Datenteilungspflicht ... 17
4. Datenkompetenz ... 18
5. Staat als Vorreiter ... 19

I. ZUSAMMENFASSUNG

- Der Verbraucherzentrale Bundesverband (vzbv) begrüßt den grundsätzlichen Tenor der Datenstrategie. Konkrete Maßnahmen, wie die Rechte der Verbraucher in einer immer stärker datengetriebenen Gesellschaft gestärkt werden können, sind jedoch nicht ausreichend enthalten.
- Eine Öffnung der Datenschutz-Grundverordnung (DSGVO) zum jetzigen Zeitpunkt ist nicht zielführend. Vielmehr sollten konsequent Instrumente weiterentwickelt, angewendet und durchgesetzt werden, mit denen auf Basis des geltenden Rechts die schutzwürdigen Interessen der Betroffenen sowie berechtigte gesellschaftliche und wirtschaftliche Interessen vereinbart werden können.
- Die Bundesregierung sollte sich im Laufe der anstehenden Trilog-Verhandlungen zur ePrivacy-Verordnung weiterhin dafür einsetzen, dass die Verbraucherinteressen gegenüber den Interessen der digitalen Werbewirtschaft und der EU-Mitgliedsstaaten nicht ins Hintertreffen geraten.
- Richtig ist die geplante Etablierung eines Forschungsnetzwerks zur Anonymisierung sowie die Förderung von Anonymisierungsverfahren und -methoden. Jedoch sind weitere gesetzgeberische Vorgaben und die Entwicklung von Standards erforderlich, mit denen konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten definiert werden.
- Der vzbv begrüßt ausdrücklich, dass sich die Bundesregierung auf EU-Ebene in den Verhandlungen zum Data Governance Act für einen rechtlichen Rahmen für Datenintermediäre einsetzen möchte. Dieser Rahmen sollte die Zulässigkeit und Grenzen von Datenintermediären regeln, Treuepflichten normieren, konfligierende Interessen ausschließen sowie entsprechende Kontroll- und Sanktionsmöglichkeiten schaffen.
- Zwar wird der hohe Stellenwert von „data protection by design“ an mehreren Stellen der Datenstrategie betont und eine Förderung anvisiert. Allerdings werden diese Absichtserklärungen nicht ausreichend in konkrete Maßnahmen, wie die Anpassung von Beschaffungsrichtlinien oder Vorgaben für die Forschungsförderung, übersetzt. Erforderlich wäre insbesondere auch eine verpflichtende und bußgeldbewehrte Adressierung der Hersteller von Webbrowsern im Rahmen der ePrivacy-Verordnung.
- Die Bundesregierung sollte sich im Austausch mit Unternehmen, Aufsichtsbehörden und Vertretern der Zivilgesellschaft für branchenbezogene Verhaltensregeln und Standards einsetzen, wie die Datenübertragbarkeit einheitlich, praktikabel und im Sinne aller Beteiligten umgesetzt werden kann.
- Die Bundesregierung sollte sich auf europäischer Ebene dafür einsetzen, dass die Datenschutzaufsichtsbehörden angemessen ausgestattet werden und das Datenschutzrecht konsequent durchsetzen. Auch muss sie gegenüber der EU-Kommission darauf drängen, dafür erforderliche unionsrechtliche Schritte einzuleiten.
- Der vzbv begrüßt, dass die Bundesregierung prüfen möchte, wie Risiken begrenzt werden können, die durch den Einsatz von algorithmenbasierten Entscheidungssystemen entstehen können. Diese Absicht ist jedoch nicht ausreichend. Vielmehr sollte die Bundesregierung die konkreten Maßnahmen zur Algorithmenkontrolle aufgreifen, die die Datenethikkommission im Jahr 2019 vorgeschlagen hat.

- Die Bundesregierung sollte sich für verpflichtende IT-Sicherheitsstandards digitaler Verbraucherprodukte auf europäischer Ebene einsetzen. Die bestehenden Regelungen und vorliegenden Entwürfe sind aus Verbrauchersicht nicht hinreichend.
- Die Bundesregierung sollte das Problem gezielter Verbrauchermanipulationen mit konkreten Maßnahmen adressieren und auf eine „Fairness-by-Design“-Pflicht für Unternehmen hinarbeiten. Diese sollte Unternehmen verpflichten, ausgewogene Entscheidungsarchitekturen zu verwenden, die es Verbrauchern ermöglichen, wirklich freie Entscheidungen nach ihren Präferenzen zu treffen.
- Es ist erfreulich, dass die Bundesregierung prüft, ob auf besonders datengetriebenen Märkten eine Verpflichtung zum Teilen von bestimmten Daten erforderlich ist. Jedoch muss eine „Pflicht zur Datenteilung“ so gestaltet werden, dass Wettbewerbsvorteile und Marktmacht großer datenverarbeitender Unternehmen und Plattformen gegenüber kleinen und mittleren Unternehmen nicht weiter verstärkt werden. Außerdem müssen bei einem möglichen Zugriff auf personenbezogene Daten alle datenschutzrechtlichen Vorgaben zwingend beachtet werden.
- Eine bundesweite Bildungsplattform muss von unabhängiger Seite kritisch begleitet werden, um Interoperabilität zu bestehenden Angeboten zu gewährleisten und Qualitätskriterien für Methoden und Lernangebote und -inhalte zu etablieren, die einen Unterricht frei von wirtschaftlichen Interessen gewährleisten können. Auf der Ebene der Prüfung und Verfügbarmachung von Unterrichtmaterialien sollten die Erkenntnisse des Materialkompasses des vzbv berücksichtigt werden.
- Die Bundesregierung sollte offene Standards und Software fördern, beispielsweise indem diese Aspekte künftig bei Vergaben der öffentlichen Hand als Vergabekriterium aufgenommen werden. Darüber hinaus sollte öffentlich finanzierte Software grundsätzlich auch der Allgemeinheit zur Verfügung gestellt werden.

II. EINLEITUNG

Mit ihrer im Januar 2021 vorgelegten Datenstrategie[1] möchte die Bundesregierung die innovative und verantwortungsvolle Datenbereitstellung und Datennutzung signifikant erhöhen. Als Voraussetzung dafür sollen Dateninfrastrukturen geschaffen, eine innovative und verantwortungsvolle Datennutzung gesteigert, die Datenkompetenz erhöht und der Staat zum Vorreiter gemacht werden.

Der vzbv begrüßt diese Initiative sowie die grundsätzliche Ausrichtung der Datenstrategie. Moderne Formen der Datenverarbeitung können ein großer Gewinn für einzelne Verbraucherinnen und Verbraucher[2] sein und zur Lösung gesellschaftlicher Probleme beitragen. Auf der anderen Seite können sie aber auch genauso große Gefahren bergen. Aus Sicht des vzbv sind eine verantwortungsvolle Datennutzung sowie das Recht der Menschen auf den Schutz ihrer personenbezogenen Daten kein Widerspruch, sondern zwei Seiten derselben Medaille. Jedoch ist es von grundlegender Bedeutung, dass durch den Wunsch, Daten besser verfügbar zu machen, datenschutzrechtliche Grundprinzipien nicht unterlaufen werden. Stets muss die Verarbeitung von personenbezogenen Daten auf eine geeignete Rechtsgrundlage gestellt werden. Außerdem muss bei der Verarbeitung personenbezogener Daten weiterhin der Grundsatz gelten, dass diese Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.

Daher ist es richtig, dass die Bundesregierung in ihrer Datenstrategie Datennutzung und Datenschutz nicht gegeneinander ausspielt, sondern nach Wegen sucht, auf der einen Seite die Chancen der Digitalisierung zu realisieren und auf der anderen Seite ihre Risiken zu adressieren. Insbesondere begrüßt der vzbv, dass die Bundesregierung davon absieht, über umstrittene Begriffe wie „Datenreichtum“, „Datensouveränität“ oder über das Konzept eines „Dateneigentums“ einen Gegenpol zum Datenschutz aufzubauen, sondern sich zu einem starken Datenschutz und der europäischen DSGVO[3] bekennt.

Der vzbv bedankt sich für die Gelegenheit, im Rahmen der Anhörung des Ausschusses Digitale Agenda des Deutschen Bundestags zur Datenstrategie der Bundesregierung sowie zu weiteren mit der Digitalisierung verbundenen Fragen Stellung nehmen zu können. Jedoch bedauert der vzbv angesichts des sehr umfangreichen Fragekatalogs die äußerst kurze Kommentierungsfrist von nur wenigen Tagen, sodass im Rahmen dieser Stellungnahme lediglich auf die drängendsten Themenbereiche eingegangen werden kann.

---

[1] Bundeskanzleramt: Datenstrategie der Bundesregierung. Kabinettfassung, 27. Januar 2021 (2021), URL: https://www.bundesregierung.de/resource/blob/992814/1845634/5bae389896531854c579069f9a699a8f/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1 [Zugriff: 18.02.2021].

[2] Die im weiteren Text gewählte männliche Form bezieht sich immer zugleich auf Personen aller Geschlechter. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

III. POSITIONEN IM EINZELNEN

1. ALLGEMEIN

1.1 Ziele und Ausrichtung der Datenstrategie

Der vzbv begrüßt das Ziel der Bundesregierung, unter Beachtung des Datenschutzrechts, die Bereitstellung von Daten zu verbessern, indem die langfristige Verfügbarkeit von Daten technisch und rechtlich sichergestellt werden soll. Insbesondere ist der grundlegende Tenor der Strategie erfreulich, mit dem vor allem in den Problemanalysen in angemessener Weise sowohl Chancen als auch Risiken der Digitalisierung thematisiert werden. Den treffenden Problembeschreibungen stehen jedoch zum Teil deutlich schwächere Zielformulierungen gegenüber, die die angesprochenen Probleme bei der Realisierung der Chancen beziehungsweise der Vermeidung von Risiken der Digitalisierung nicht ausreichend adressieren.

> Vor allem sind jedoch die aufgeführten konkreten Maßnahmen der Bundesregierung aus Verbrauchersicht vielfach enttäuschend. Statt die formulierten Ziele konsequent zu verfolgen, erscheinen sie vielmehr als eine Auflistung digitalpolitischer Vorhaben, die in den verschiedenen Ressorts unabhängig der Strategie ohnehin vorgesehen waren.

Ein großer Teil der Maßnahmen beinhaltet darüber hinaus lediglich die alternativlose Umsetzung von EU-Gesetzgebungen in deutsches Recht, unverbindliche Absichtserklärungen und Prüfaufträge, Ankündigungen von Forschungsvorhaben sowie Instrumente der Wirtschaftsförderung. Maßnahmen, wie die Rechte der Verbraucher in einer immer stärker datengetriebenen Gesellschaft gestärkt werden können, sind in der Datenstrategie nicht ausreichend enthalten. Hierzu hatte die Datenethikkommission (DEK) der Deutschen Bundesregierung im Oktober 2019 eine Vielzahl von Handlungsempfehlungen vorgestellt,[4] die allerdings von der Bundesregierung – auch in der Datenstrategie – nur schleppend aufgegriffen und umgesetzt wurden (wie etwa hinsichtlich der Anonymisierung personenbezogener Daten oder der Algorithmenkontrolle).[5]

Bedauerlich ist außerdem, dass aufgrund des späten Zeitpunkts der Vorlage der Datenstrategie kaum mehr die Möglichkeit besteht, noch in dieser Legislaturperiode konkrete gesetzgeberische Initiativen anzustoßen. Umso mehr verwundert es, dass eine stringente Überprüfung der Maßnahmen bis auf weiteres nicht vorgesehen ist.

1.2 „Verantwortungsvolle“ und „innovative“ Datennutzung

Es ist positiv, dass die Bundesregierung der Datenstrategie eine Erläuterung voranstellt, was unter einer verantwortungsvollen Datennutzung zu verstehen ist. Die entsprechenden Ausführungen sind klar zu begrüßen. Der vzbv stimmt zu, dass in einer

---

[4] Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission (2019), URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf [Zugriff: 18.02.2021].

[5] Siehe auch Verbraucherzentrale Bundesverband (vzbv): Umsetzung der Empfehlungen der Datenethikkommission (2020), URL: https://www.vzbv.de/pressemitteilung/bundesregierung-enttaeuscht-bei-regulierung-von-algorithmen [Zugriff: 18.02.2021].

digitalen Gesellschaft stets der Mensch im Mittelpunkt stehen muss, wofür auch das europäische Datenschutzrecht eine wesentliche Rolle spielt. Der vzbv ist außerdem der Ansicht, dass eine „verantwortungsvolle Nutzung“ nicht mit einer „rechtskonformen Nutzung“ deckungsgleich sein kann. Es sollte sichergestellt werden, dass eine „verantwortungsvolle Nutzung“ stets eine gemeinwohlorientierte Perspektive aufweist.

> Es ist demgegenüber jedoch bedauerlich, dass die Bundesregierung nicht definiert, was unter dem Schlagwort der „innovativen“ Datennutzung zu verstehen ist. So sind beispielsweise Geschäftsmodelle, die alleine darauf ausgerichtet sind, Nutzerdaten zu Werbezwecken zu kommerzialisieren oder Verbraucher zu kommerziellen Zwecken zu beeinflussen, nach Ansicht des vzbv nicht als innovativ zu betrachten.

2. DATENINFRASTRUKTUR

Aufgrund der Vielzahl der vorgelegten Fragen sowie der kurzen Antwortfrist, ist es dem vzbv nicht möglich, zu diesem Themenkomplex Stellung zu beziehen.

3. DATENNUTZUNG

3.1 Regelungsbedarf im Datenschutzrecht

Auch wenn der vzbv durchaus weiteren Regelungsbedarf im europäischen Datenschutzrecht erkennt, um die Rechte und Freiheiten der Verbraucher umfassend zu schützen[6], sind aktuelle Debatten um eine Öffnung der DSGVO zum jetzigen Zeitpunkt nicht zielführend.

Auf der einen Seite ist die öffentliche Diskussion vor allem von Kritik und Klagen über Schwierigkeiten bei der Anwendung der DSGVO geprägt. Viele der Klagen sind berechtigt. Einige Diskussionsbeiträge zielen jedoch auf eine grundsätzliche Abschwächung des europäischen Datenschutzrechts ab, was nach Ansicht des vzbv die völlig falsche Antwort auf die Herausforderungen der Digitalisierung wäre. Es ist unvermeidbar, dass die praktische Umsetzung eines solch umfassenden Gesetzes erst einmal vor allem als Last wahrgenommen wird. Jedoch hat sich auch gezeigt, dass sich viele der anfangs geäußerten Befürchtungen – wie beispielsweise massive Abmahnwellen – nicht realisiert haben. Vielmehr entwickelt die DSGVO als Erfolgsmodell eine positive Ausstrahlungskraft über Europa hinaus und gilt als Maßstab für Datenschutzgesetzgebungen anderer Staaten.

Insbesondere ist es jedoch nicht realistisch, dass bei einer Öffnung der DSGVO lediglich kleinere Anpassungen vorgenommen werden – im Gegenteil würde dies zu einer erneuten, umfassenden Aushandlung des mühsam gefundenen Kompromisses führen.

[6] Siehe auch Verbraucherzentrale Bundesverband: Evaluation der DSGVO aus Sicht der Verbraucher (2019), URL: https://www.vzbv.de/sites/default/files/downloads/2019/12/04/19-11-27_vzbv-positionspapier_evaluation_dsgvo.pdf [Zugriff: 18.02.2021].

> Es sollten daher konsequent Instrumente weiterentwickelt, angewendet und durchgesetzt werden, mit denen auf Basis des geltenden Rechts die schutzwürdigen Interessen der Betroffenen sowie berechtigte gesellschaftliche und wirtschaftliche Interessen vereinbart werden können. Viele dieser Instrumente wurden bereits von der DEK empfohlen sowie in der Datenstrategie der Bundesregierung angerissen und werden in den folgenden Kapiteln dieser Stellungnahme aus der Perspektive des vzbv ausgeführt.

Dringender Regelungsbedarf besteht nach Auffassung des vzbv jedoch hinsichtlich des Datenschutzes und der Vertraulichkeit in der elektronischen Kommunikation. Aus Sicht der Verbraucher muss gewährleistet sein, dass der Schutz persönlicher Daten und die Vertraulichkeit in den derzeitigen Verhandlungen zur europäischen ePrivacy-Verordnung im Vordergrund stehen und nicht verhandelbar sind. Aus Verbrauchersicht ist die Position der europäischen Mitgliedsstaaten[7] daher ein Skandal. Diese bleibt nicht nur weit hinter den Entwürfen der Europäischen Kommission und des Europäischen Parlaments zurück, vielmehr schränkt sie den Datenschutz und die Vertraulichkeit der elektronischen Kommunikation massiv ein und zerstört so das Vertrauen der Verbraucher.[8]

> Die Bundesregierung sollte sich daher im Laufe der anstehenden Trilog-Verhandlungen weiterhin dafür einsetzen, dass die Verbraucherinteressen gegenüber den Interessen der digitalen Werbewirtschaft und der EU-Mitgliedsstaaten nicht ins Hintertreffen geraten.

3.2 Anonymisierung

Die Weiterentwicklung von Anonymisierungstechniken ist ein wesentlicher Baustein, um die Ziele der Datenstrategie zu erreichen. Eine einwandfreie Anonymisierung stellt jedoch eine überaus anspruchsvolle Herausforderung dar, insbesondere wenn Daten über einen unbestimmten Zeithorizont mit unbestimmten Empfängern geteilt oder gar veröffentlicht werden und somit aus verschiedenen Quellen zusammengeführt werden können. Seit einigen Jahren wird verstärkt daran geforscht, wie mit entsprechenden Sicherheitskonzepten eine starke Anonymisierung erreicht werden kann, ohne dass die Analysequalität leidet.

> Daher ist es richtig, dass die Bundesregierung ein Forschungsnetzwerk zur Anonymisierung etablieren sowie Anonymisierungsverfahren und -methoden fördern möchte.

Diese Maßnahmen sind jedoch nicht ausreichend. So hat der europäische Gesetzgeber in der DSGVO Abstand von einem absoluten Anonymisierungsbegriff genommen. Anonymisierung ist demnach nicht binär zu verstehen, vielmehr gibt es ein Spektrum

[7] Council of the European Union: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (2021), URL: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf [Zugriff: 18.02.2021].

[8] Siehe auch Verbraucherzentrale Bundesverband (vzbv): Grundrechte in Gefahr (2021), URL: https://www.vzbv.de/pressemitteilung/grundrechte-gefahr [Zugriff: 18.02.2021].

verschiedener Anonymisierungsmaßnahmen, die unterschiedliche Qualitäten aufweisen und somit für verschiedene Zwecke unterschiedlich angemessen und geeignet sind. Die DSGVO gibt jedoch keine Auskunft darüber, unter welchen Umständen eine Anonymisierung als hinreichend erachtet werden kann.

> Um Unternehmen beim Einsatz der Anonymisierung weiter zu unterstützen, sollte sich die Bundesregierung dafür einsetzen, dass Wirtschaft und Aufsichtsbehörden gemeinsam Kriterien für die Frage entwickeln, welche Anonymisierungsmaßnahmen in bestimmten Kontexten als ausreichend betrachtet werden können, um die Risiken der Identifizierbarkeit, Aussonderung, Verkettbarkeit und Inferenz einzelner Betroffener auszuschließen. [9]

Der vzbv begrüßt darüber hinaus, dass die Bundesregierung auch Risiken in den Fokus nehmen möchte, die durch Auswertung aggregierter/anonymer/synthetischer Daten entstehen können und entsprechende rechtliche Rahmenbedingungen in Erwägung zieht.

> Nach Ansicht des vzbv sind gesetzgeberische Vorgaben und die Entwicklung von Standards dringend erforderlich, mit denen konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten definiert werden. Dies sollte um strafbewehrte Verbote der De-Anonymisierung ergänzt werden.[10]

Beispiele für weiterführende Schutzkonzepte finden sich im außereuropäischen Ausland. So wurde beispielsweise in Japan das Konzept der „anonymously processed information“ (API) eingeführt.[11] Für die Erstellung solcher Informationen gelten weitreichende Anforderungen, die eine De-Anonymisierung unmöglich machen oder zumindest wesentlich erschweren sollen. Auch nach der Anonymisierung müssen die Verantwortlichen weitere Sicherheitsmaßnahmen ergreifen. Darüber hinaus wurde es verboten, anonymisierte Daten mit anderen Daten zusammenzuführen, um den Personenbezug wiederherzustellen, sowie im Anonymisierungsverfahren entfernte, aber noch andernorts vorhandene Merkmale zu erwerben. Ferner wurden Informationspflichten gegenüber der Öffentlichkeit eingeführt, unter anderem in Bezug auf die Kategorien von Informationen, die in den anonymisierten Daten enthalten sind.

---

[9] Siehe auch Verbraucherzentrale Bundesverband: Anonymisierung unter der DSGVO (2020), URL: https://www.vzbv.de/sites/default/files/downloads/2020/03/24/20-03-20_bfdi_vzbv-stellungnahme_anonymisierung.pdf [Zugriff: 18.02.2021].

[10] Vgl. Roßnagel, Alexander; Geminn, Christian: Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht. Gutachten im Auftrag des vzbv (2019), S. 96f, URL: https://www.vzbv.de/sites/default/files/downloads/2019/12/04/19-11-26_gutachten_evaluation_dsgvo.pdf [Zugriff: 18.02.2021].; Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 4), S. 129ff.

[11] Vgl. Geminn, Christian; Laubach, Anne; Fujiwara, Shizuo: Schutz anonymisierter Daten im japanischen Datenschutzrecht (2018), in: ZD, S. 413–420, URL: https://beck-online.beck.de/Bcid/Y-300-Z-ZD-B-2018-S-413-N-1 [Zugriff: 18.02.2021].

3.3 Datenintermediäre

Durch die Etablierung von Datenintermediären könnte Verbrauchern bessere Kontrollmöglichkeiten über ihre Daten an die Hand gegeben und damit das Vertrauen in die Digitalisierung und die datenverarbeitende Wirtschaft gestärkt werden.[12] Gleichzeitig könnten Unternehmen auf eine größere Datenbasis mit einer besseren Datenqualität zugreifen, was wiederum die Qualität ihrer Analysen und der Forschung verbessern würde. Nicht zuletzt würde sich die Rechtssicherheit der Datenverarbeitung erhöhen, da zum Beispiel Einwilligungen leichter entsprechend datenschutzrechtlicher Vorgaben eingeholt werden könnten.

Doch auch wenn Datenintermediäre die digitale Selbstbestimmung des Einzelnen fördern sollen, können von ihnen große Gefahren ausgehen. So sieht beispielsweise die DEK das Risiko, dass Verbraucher auf einen Weg der unbewussten oder sorglosen Fremdbestimmung geführt werden könnten. Insbesondere würde es der Idee der Datenintermediäre widersprechen, wenn Entscheidungen von Betroffenen an die Betreiber abgegeben oder Entscheidungen Betroffener durch diese interessenwidrig beeinflusst werden.[13] Kritisch ist in diesem Zusammenhang beispielsweise, dass im Arbeitspapier „Datenmanagement- und Datentreuhandsysteme“ der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2020 das Transparency & Consent Framework des Branchenverbands IAB Europe[14] als Positivbeispiel für Einwilligungsmanagement-Dienste angeführt wird.[15] Dieses IAB-Framework widerspricht jedoch nach Ansicht europäischer Datenschutzbeauftragter den Anforderungen der DSGVO.[16] Dies zeigt, wie wichtig eine strenge Kontrolle darüber ist, welche Organisationen als Datenintermediäre agieren dürfen, um Verbraucher nicht einem Risiko auszusetzen.

Von überragender Bedeutung ist insbesondere, dass mögliche Interessenkonflikte zwischen Datenintermediären und Datengebern ausgeschlossen werden, die trotz einer Ansiedlung der Dienste bei einer gesonderten Rechtsperson bestehen können. Ein Beispiel für mögliche Interessenkonflikte ist der Dienst Verimi, dessen Gesellschafter Unternehmen wie Allianz, Axel Springer, die Bundesdruckerei, Daimler, die Deutsche Bahn, die Deutsche Bank, die Deutsche Telekom, die Lufthansa, Samsung sowie Volkswagen Financial Services sind. Anfangs wurde der Dienst Verbrauchern gegenüber als datenschutzfreundliche Alternative zu den Single-Sign-On-Angeboten von Facebook und Google sowie als Dienst zum Einwilligungsmanagement beworben. Innerhalb der digitalen Werbewirtschaft galt der Dienst jedoch als Lösung, um sich gegen die strengen Anforderungen der kommenden ePrivacy-Verordnung an eine Einwilligung

---

[12] Siehe auch Verbraucherzentrale Bundesverband: Neue Datenintermediäre (2020), URL: https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf [Zugriff: 18.02.2021].

[13] Vgl. auch Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 4), 133f.

[14] IAB Europe: TCF - Transparency & Consent Framework (2018), URL: https://iabeurope.eu/transparency-consent-framework/ [Zugriff: 18.02.2021].

[15] Vgl. Fokusgruppe Datenschutz des Digital-Gipfels 2020: Datenmanagement- und Datentreuhandsysteme (2020), S. 11, URL: https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2020/p9-datenmanagement-und-datentreuhandsysteme.pdf [Zugriff: 18.02.2021].

[16] Vgl. Irish Council for Civil Liberties: Data Protection Authority investigation finds that the IAB Transparency and Consent Framework infringes the GDPR. (2020), URL: https://www.iccl.ie/human-rights/info-privacy/apd-iab-findings/ [Zugriff: 23.12.2020].

für das Tracking im Internet zu wappnen.[17] Nach in der Presse zitierten Äußerungen von Verimi-Mitarbeitern soll sich dieser Ansatz zwar nicht durchgesetzt haben,[18] der Fall zeigt jedoch mögliche Interessenkonflikte auf.

> Der vzbv begrüßt ausdrücklich, dass sich die Bundesregierung auf EU-Ebene in den Verhandlungen zum Data Governance Act für einen rechtlichen Rahmen für Datenintermediäre einsetzen möchte. Dieser Rahmen sollte die Zulässigkeit und Grenzen von Datenintermediären regeln, Treuepflichten normieren, konfligierende Interessen ausschließen sowie entsprechende Kontroll- und Sanktionsmöglichkeiten schaffen.[19]

3.4 Datenschutz durch Technikgestaltung

Zwar wird der hohe Stellenwert von Datenschutz durch Technikgestaltung und Voreinstellungen („data protection by design“) an mehreren Stellen der Datenstrategie betont und eine Förderung anvisiert. Allerdings werden diese guten Absichtserklärungen nicht ausreichend in konkrete Maßnahmen übersetzt – wie etwa die lediglich als Ziele formulierte Anpassung von Beschaffungsrichtlinien oder Vorgaben für die Forschungsförderung. Gleiches gilt für die Förderung datenschutzkonformer Angebote auf dem Markt.

Problematisch ist weiterhin, dass Regelungsadressat der DSGVO lediglich die datenverarbeitenden Stellen sind, nicht jedoch die Hersteller von Produkten und Software. Dabei sind es vor allem die Hersteller, die über Gestaltungsspielräume hinsichtlich der datenschutzkonformen Technikgestaltung der Produkte verfügen.[20] „Dies führt dazu, dass sich letztlich stets derjenige durchsetzt, der die Technikgestaltung durchführt, ohne dass Art. 25 DSGVO den Verbrauchern einen Anspruch verleiht, mehr zu verlangen. Eine verpflichtende und bußgeldbewehrte Adressierung der Hersteller wäre weitaus effektiver und würde die Vorschrift nicht lediglich auf einen wohlgemeinten Programmsatz reduzieren.“[21]

Besonders deutlich tritt dieser Mangel bei Software zu Tage, die den Abruf von Informationen aus dem Internet oder eine elektronische Kommunikation erlaubt, wie beispielsweise Webbrowsern.[22] Das Flash Eurobarometer 443 der EU-Kommission zeigt eindeutig, dass sich die Verbraucher datenschutzfreundliche Voreinstellungen wünschen. In dieser Studie hatten sich 90 Prozent der deutschen Internetnutzer für solche

---

[17] Vgl. Günther, Vera: Datenschutz und Datenallianzen. in: Horizont (2018), URL: https://www.horizont.net/medien/nachrichten/Datenschutz-und-Datenallianzen-Wenn-wir-nicht-reagieren-fliessen-noch-mehr-Gelder-nach-Amerika-164094 [Zugriff: 18.02.2021].

[18] Vgl. Bröckling, Marie: Eine Identität für alles: Das schwierige Geschäftsmodell von Verimi. in: Netzpolitik.org (2018), URL: https://netzpolitik.org/2018/eine-identitaet-fuer-alles-das-schwierige-geschaeftsmodell-von-verimi/ [Zugriff: 18.02.2021].

[19] Siehe auch Verbraucherzentrale Bundesverband: Vertrauen stärken durch verbraucherfreundliche Daten-Governance (2021), URL: https://www.vzbv.de/sites/default/files/downloads/2021/01/13/21-01-12_vzbv-stellungnahme_data-governance-act.pdf [Zugriff: 18.02.2021].

[20] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 4), S. 119f.

[21] Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 10), S. 51.

[22] Siehe auch Verbraucherzentrale Bundesverband: Datenschutz und Privatsphäre bei Telekommunikationsdiensten und Telemedien sicherstellen (2021), URL: https://www.vzbv.de/sites/default/files/downloads/2021/01/22/21-01-21_vzbv-stellungnahme_ttdsg-e.pdf [Zugriff: 18.02.2021].

Voreinstellungen in ihren Webbrowsern ausgesprochen.[23] Gleichzeitig zeigt die Studie auch, dass besonders ältere Menschen, Menschen mit niedriger Bildung sowie Menschen, die das Internet wenig verwenden, seltener Änderungen in den Datenschutzeinstellungen ihrer Software vornehmen.[24] Datenschutzfreundliche Voreinstellungen schützen also in erster Linie diese besonders vulnerablen Verbrauchergruppen.

Die ePrivacy-Verordnung, die derzeit in Brüssel verhandelt wird, wäre der richtige Ort, um solche Vorgaben zu verankern. Besonders das Europäische Parlament hat hierfür gute Vorschläge gemacht.[25]

> Der vzbv bedauert daher sehr, dass der entsprechende Regelungsvorschlag der EU-Kommission im Rahmen der Verhandlungen im EU-Rat ersatzlos gestrichen wurde.[26] Die Bundesregierung sollte sich auch weiterhin für dessen Wiederaufnahme einsetzen.

3.5 Datenübertragbarkeit

Grundsätzlich kann das Recht auf Datenübertragbarkeit die Kontrolle der Verbraucher über ihre Daten stärken sowie marktbeherrschende Stellungen von Unternehmen verringern beziehungsweise stärkeren Wettbewerb ermöglichen. Entsprechend der DSGVO haben betroffene Personen das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

Problematisch ist jedoch, dass die Anforderungen an ein „strukturiertes, gängiges und maschinenlesbares Format“ in der Praxis bislang noch sehr unterschiedlich und uneinheitlich ausgelegt werden, obwohl sie Grundvoraussetzung für eine wirkungsvolle Ausübung des Portabilitätsrechts sind.[27] In einer Untersuchung von acht Diensten sozialer Medien hat der Marktwächter Digitale Welt der Verbraucherzentralen und des vzbv die Ausübung des Rechts auf Datenübertragbarkeit getestet.[28] Zwar wurden Datensätze zur Verfügung gestellt, allerdings lagen diese nur in sehr unterschiedlichen Dateiformaten vor und waren mit Standardsoftware meist nicht zu öffnen. Die Daten waren für Verbraucher damit nicht überprüfbar. Kritisiert wurde, dass Verbraucher keine informierte Entscheidung darüber treffen konnten, ob die Daten zutreffend waren und welche Daten bei einem Wechsel zum neuen Anbieter übertragen werden sollten.

Diese Marktwächteruntersuchung zeigt, dass noch viele Fragen in der praktischen Anwendung der Datenübertragbarkeit offen sind. Eine einheitliche Praxis wäre jedoch sowohl im Interesse der Verbraucher als auch der Unternehmen.

---

[23] Vgl. Europäische Kommission: Flash Eurobarometer 443 (2016), S. 46, URL: https://data.europa.eu/euodp/en/data/dataset/S2124_443_ENG [Zugriff: 18.02.2021].

[24] Vgl. ebd., S. 37.

[25] Vgl. Entwurf einer legislativen Entschließung des Europäischen Parlaments vom 23.10.2017, A8-0324/2017.

[26] Vgl. Council of the European Union (2021) (wie Anm. 7).

[27] Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 4), S. 136.

[28] Marktwächter Digitale Welt: Soziale Medien und die EU-Datenschutzgrundverordnung - Teil 2 (2018), URL: https://www.vzbv.de/sites/default/files/downloads/2020/01/20/bericht_soziale_medien_dsgvo.pdf [Zugriff: 18.02.2021].

Die Bundesregierung sollte sich daher im Austausch mit Unternehmen, Aufsichtsbehörden und Vertretern der Zivilgesellschaft für branchenbezogene Verhaltensregeln und Standards einsetzen, wie die Datenübertragbarkeit einheitlich, praktikabel und im Sinne aller Beteiligten umgesetzt werden kann.

3.6 Datenschutzaufsicht

Die Durchsetzung der DSGVO in Europa verläuft insbesondere gegenüber den großen Unternehmen der Digitalwirtschaft unbefriedigend. So haben beispielsweise im November 2018 verschiedene europäische Verbraucherschutzorganisationen bei ihren jeweiligen nationalen Datenschutzbehörden Beschwerden gegen die Standortverfolgungspraktiken von Google eingelegt, die nach ihren Erkenntnissen gegen die DSGVO verstoßen. Anschließend dauerte es neun Monate, bis Juli 2019, bevor die irische Datenschutzbehörde zur federführenden Behörde für die Beschwerden ernannt wurde. Es dauerte weitere sechs Monate bis Februar 2020, bis die Behörde die Eröffnung einer Untersuchung zu den in den Beschwerden aufgeworfenen Verstößen ankündigte und ein Verfahren einleitete. Bis heute ist weiterhin unklar, wann eine Entscheidung der Aufsichtsbehörde zu erwarten ist.[29] Gleiches gilt für eine Vielzahl ähnlich gelagerter Fälle, besonders wenn diese in den Zuständigkeitsbereich der irischen und luxemburgischen Aufsichtsbehörden fallen.

Das Beispiel zeigt, dass einzelne europäische Datenschutzbehörden entweder Unwillens oder unfähig sind, die DSGVO angemessen durchzusetzen. Dies schränkt nicht nur die Rechte der Verbraucher ein, sondern führt auch zu der berechtigten Kritik von deutschen Unternehmen, warum hier mit zweierlei Maß gemessen wird.

Die Bundesregierung sollte sich daher – im Interesse der deutschen Verbraucher und der deutschen Wirtschaft – auf europäischer Ebene dafür einsetzen, dass die europäischen Aufsichtsbehörden angemessen ausgestattet werden und das Datenschutzrecht konsequent durchsetzen. Auch muss sie gegenüber der EU-Kommission darauf drängen, dafür erforderliche unionsrechtliche Schritte einzuleiten.

Auch in Deutschland hat die DSGVO zu einer deutlichen Ausweitung der Aufgaben der Datenschutzaufsichtsbehörden geführt. Außerdem hat sich seit Anwendung der DSGVO die Anzahl von Beschwerden sowie die Meldung von Datenschutzverstößen massiv erhöht. Zwar wurden auch die personellen und finanziellen Ressourcen der Aufsichtsbehörden in den vergangenen Jahren erhöht, jedoch ist diese weiterhin nicht ausreichend, um den genannten Anforderungen angemessen gerecht zu werden.[30] Gleichzeitig wird vielfach der berechtigte Wunsch geäußert, dass die Aufsichtsbehörden über ihre eigentlichen Aufgaben hinaus, Unternehmen verstärkt in Datenschutzfragen beraten sollten.

[29] Vgl. Bureau Européen des Unions de Consommateurs (BEUC): Commercial surveillance by Google. Long delay in GDPR complaints, URL: https://www.beuc.eu/press-media/news-events/commercial-surveillance-google-long-delay-gdpr-complaints [Zugriff: 18.02.2021].

[30] Vgl. Roßnagel, Alexander; Geminn, Christian (2019) (wie Anm. 10), S. 52ff.

> Dementsprechend sollte sich die Bundesregierung gegenüber den Bundesländern für eine bessere Ausstattung der Datenschutzaufsichtsbehörden einsetzen.

Derzeit mehren sich außerdem Debattenbeiträge, die eine Neustrukturierung der deutschen Datenschutzaufsicht fordern. Auch der vzbv mahnt an, dass eine kohärente Datenschutzaufsicht sichergestellt werden muss. Die Herstellung von Nachvollziehbarkeit, Verbindlichkeit und Einheitlichkeit der Auslegung der DSGVO ist im Interesse der Verbraucher. Diese Verbindlichkeit ist in Deutschland (anders als auf EU-Ebene) bisher nicht gegeben, da die Datenschutzkonferenz (DSK) keine institutionell verankerte Organisation ist (wie etwa der Europäische Datenschutzausschuss), sondern ein inoffizielles Zusammenkommen der Datenschutzaufsichtsbehörden. Auch wäre es im Sinne der Verbraucher, wenn die DSK schneller zu gemeinsamen Ergebnissen kommen würde.

Ein derzeit diskutierter Vorschlag sieht daher vor, sich für die DSK an den Vorgaben zu orientieren, die die DSGVO für den europäischen Datenschutzausschuss – insbesondere zu verbindlichen Mehrheitsentscheidungen – macht. Verfahrensdetails könnten über einen Bund-Länder-Staatsvertrag geregelt werden.[31] Jedoch muss dabei in Betracht gezogen werden, dass auch der Kohärenzmechanismus des europäischen Datenschutzausschusses durchaus Schwächen hat, wie beispielsweise die unzufrieden stellende Durchsetzung der DSGVO gegenüber in Irland und Luxemburg ansässigen Unternehmen zeigt.

> Der vzbv hält den Vorschlag grundsätzlich für diskussionswürdig. Allerdings sollte zuerst geprüft werden, ob nicht bereits mit einer besseren Ausstattung der Aufsichtsbehörden und einer stärkeren Institutionalisierung der DSK, zum Beispiel unter anderem durch eine eigene Geschäftsstelle, eine Verbesserung der Harmonisierung erreicht werden kann, bevor neue (rechtliche) Strukturen geschaffen werden. Diese Option dürfte auch in deutlich kürzerer Zeit zu erreichen sein, als die Entwicklung eines deutschen Kohärenzmechanismus.

> Ein neues Innovationsboard auf EU-Ebene als Ansprechpartner für Datenschutzfragen, wie in der Datenstrategie der Bundesregierung vorgeschlagen, lehnt der vzbv klar ab. Für diese Aufgabe müssen – auch im Sinne der Rechtssicherheit – weiterhin die Datenschutzaufsichtsbehörden und der Europäische Datenschutzausschuss zuständig sein.

3.7 Algorithmenbasierte Entscheidungssysteme

Eng verbunden mit einer verantwortungsvollen Datennutzung ist die Frage, welche Anforderungen an algorithmenbasierte Entscheidungssysteme gestellt werden müssen. Denn diese werden künftig eine zentrale Funktion bei der Verarbeitung von Daten einnehmen. Daher begrüßt der vzbv im Grundsatz, dass die Bundesregierung prüfen

[31] Vgl. Schaar, Peter: Datenschutz besser koordinieren und effektiver durchsetzen (2020), URL: https://www.eaid-berlin.de/datenschutz-besser-koordinieren-und-effektiver-durchsetzen/ [Zugriff: 18.02.2021].

möchte, wie Risiken begrenzt werden können, die durch den Einsatz von algorithmenbasierten Entscheidungssystemen (wie KI) entstehen können. Auch begrüßt der vzbv die kritische Auseinandersetzung der Bundesregierung mit dem Profiling und Scoring der Verbraucher. Jedoch sind die Maßnahmen zur Begrenzung der von der Bundesregierung benannten Risiken unzureichend.[32] Vielmehr sollte die Bundesregierung über eine reine Prüfung die konkreten Maßnahmen zur Algorithmenkontrolle aufgreifen, die die DEK bereits im Jahr 2019 vorgeschlagen hat.

> Die Bundesregierung sollte unter anderem ein bundesweites Kompetenzzentrum für algorithmische Systeme schaffen, welches in der Lage ist, die zuständigen Aufsichtsbehörden bei der Prüfung der Rechtmäßigkeit und der gesellschaftlichen Auswirkungen von Anwendungen zu unterstützen. Ein Kompetenzzentrum, dass sich alleine auf „KI in der öffentlichen Verwaltung“ bezieht, wie in Kapitel 4 der Datenstrategie vorgeschlagen, ist nicht ausreichend.[33]

> In diesem Sinne sollte die Bundesregierung sich außerdem für eine Europäische Verordnung für algorithmische Systeme einsetzen. Diese Verordnung sollte einem risikoadaptierten Regulierungsansatz folgen mit horizontalen Regeln zur Gestaltung und Zulässigkeit von algorithmenbasierten Entscheidungssystemen und Künstlicher Intelligenz, zu Betroffenenrechten, Transparenz, Aufsichtsinstitutionen und -strukturen sowie technischen Vorgaben zur Absicherung der Rechtmäßigkeit der Systeme. Dies sollte durch sektorale Regeln weiter konkretisiert werden.[34]

3.8 IT-Sicherheit

Eine verantwortungsvolle Datennutzung kann nur vor dem Hintergrund eines hohen IT-Sicherheitsniveaus für Verbraucher gewährleistet werden. Um dieses ist es jedoch oftmals schlecht bestellt. Beispielsweise ist für digitale Dienste die unsichere Authentisierung mit einem Passwort nach wie vor der Normalfall.[35] Vernetzte Geräte sind oftmals gar nicht oder lediglich mit leicht herauszufindenden Passwörtern gesichert, und eine sichere Authentisierung erfolgt häufig auch nicht.[36] Viele Sicherheitsprobleme entstehen dadurch, dass Daten unverschlüsselt gespeichert und gesendet werden und Nutzerzugänge unzureichend gesichert sind. Dementsprechend könnte das Ausmaß der Risiken, denen Verbraucher im digitalen Raum und bei der Nutzung vernetzter Geräte ausgesetzt sind, mit vergleichsweise einfachen technischen Sicherheitsvorkehrungen drastisch reduziert werden.

---

[32] Siehe auch Verbraucherzentrale Bundesverband: Algorithmenkontrolle. Positionspapier des vzbv (2019), URL: https://www.vzbv.de/sites/default/files/downloads/2019/05/02/19-05-02_vzbv_positionspapier_algorithmenkontrolle.pdf [Zugriff: 18.02.2021] sowie Verbraucherzentrale Bundesverband: Weißbuch zu Künstlichen Intelligenz - Vorschläge des vzbv (2020), URL: https://www.vzbv.de/dokument/weissbuch-ki-zu-wenig-ambitioniert [Zugriff: 17.02.2020].

[33] Siehe auch Verbraucherzentrale Bundesverband (vzbv) (wie Anm. 5).

[34] Vgl. Datenethikkommission der Bundesregierung (DEK) (2019) (wie Anm. 4), S. 180ff.

[35] Bei den vielen Anbietern, beispielsweise Google, muss diese Funktion nachträglich aktiviert werden: Google: Mehr Sicherheit für Ihr Google-Konto, URL: https://www.google.com/landing/2step/ [Zugriff: 18.02.2021].

[36] T. Alladi, V. Chamola, B. Sikdar and K. R. Choo (2020): „Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, Vol. 9, Nr. 2, S. 17-25, doi: 10.1109/MCE.2019.2953740. S. 20 ff.

Daher sollten alle digitalen Dienste und vernetzten Geräte verpflichtend mit grundlegenden Sicherheitsmaßnahmen konstruiert (*Security by Design*) und den Verbrauchern übergeben werden müssen, sodass diese sie nicht erst durch umständliches Konfigurieren sicher machen müssen (*Security by Default*). Wesentliche Maßnahmen wären unter anderem die verschlüsselte Übertragung und Speicherung von Daten, der Einsatz sicherer Authentisierungsverfahren (zum Beispiel 2-Faktor-Authentisierung), der Schutz von Anwendungen und Daten mit Passwörtern auf einem angemessenen Sicherheitsniveau sowie die regelmäßige und ausreichend lange Bereitstellung von Sicherheitsupdates.

> Die Bundesregierung sollte sich daher weiterhin für verpflichtende IT-Sicherheitsstandards digitaler Verbraucherprodukte auf europäischer Ebene einsetzen. Die bestehenden Regelungen und vorliegenden Entwürfe sind aus Verbrauchersicht nicht hinreichend.[37]

Darüber hinaus bedarf es eines entsprechenden Rechtsrahmens für vernetzte Geräte als „cyberphysische Systeme“, denn die Verbindung von physischen Produkten mit vernetzten IT-Systemen führt zu gänzlich neuen Herausforderungen mit Blick auf die Cybersicherheit. Im Sinne einer „kontinuierlichen Konformität“ muss der Sicherheitsstandard zum Zeitpunkt der Inverkehrbringung durch einen Mechanismus zur Einspielung von Sicherheitsupdates des Herstellers erhalten bleiben. Einige Fragen in diesem Zusammenhang sind durch eine Modernisierung und Erweiterung der Allgemeinen Produktsicherheitsrichtlinie zu klären.[38]

3.9 Weitere Stärkung der Verbraucherrechte in der Datenökonomie

Der vzbv begrüßt, dass die Bundesregierung die Risiken von „Addictive Designs“ und „Dark Patterns“ adressiert. Bedauerlich ist allerdings, dass keine entsprechenden Maßnahmen zur Reduzierung dieser Risiken benannt wurden. Die Verwendung von "Dark Patterns" zur versteckten Beeinflussung von Verbraucherentscheidungen oder manipulative Entscheidungsarchitekturen (wie Auswahlmenüs) verzerren die Wahlmöglichkeiten der Verbraucher und drängen sie dazu, Entscheidungen zu treffen, die nicht ihren wahren Präferenzen entsprechen.[39]

---

[37] Siehe auch Verbraucherzentrale Bundesverband: Netz-und Informationssicherheit auch für Verbraucher stärken (2021), URL: https://www.vzbv.de/sites/default/files/downloads/2021/01/29/2021-01-25_vzbv_stn_nis2.pdf [Zugriff: 18.02.2021].

[38] Siehe auch dass.: Sichere Produkte stärken das Verbrauchervertrauen (2020), S. 14f, URL: https://www.vzbv.de/sites/default/files/downloads/2020/11/23/20-10-01_vzbv_positionspapier_produktsicherheit.pdf [Zugriff: 18.02.2021].

[39] Diese Taktiken sind gut dokumentiert und werden etwa eingesetzt, um Nutzer zur Einwilligung in die Datenerfassung und -verarbeitung zu drängen (vgl. Peter Hense: The end of dark patterns in “cookie walls”: German court bans deceptive designs (2021), URL: https://www.jdsupra.com/legalnews/the-end-of-dark-patterns-in-cookie-5786302/ [Zugriff: 01.02.2021]), sie bewusst davon abzuhalten, sich von Diensten abzumelden (vgl. Forbrukerradet: Amazon manipulates customers to stay subscribed, URL: https://www.forbrukerradet.no/news-in-english/amazon-manipulates-customers-to-stay-subscribed/ [Zugriff: 01.02.2021]) oder sie zum Kauf zusätzlicher Dienste zu bewegen (vgl: Sportico: Federal Law Suit: This Video Game is too Damn Hard (2020), URL: https://www.sportico.com/law/analysis/2020/ea-sports-its-in-the-game-1234617287/ [Zugriff: 01.02.2021]).

> Die Bundesregierung sollte das Problem gezielter Verbrauchermanipulationen mit konkreten Maßnahmen adressieren und auf eine „Fairness-by-Design"-Pflicht für Unternehmen hinarbeiten. Diese sollte Unternehmen verpflichten, ausgewogene Entscheidungsarchitekturen zu verwenden, die es Verbrauchern ermöglichen, wirklich freie Entscheidungen nach ihren Präferenzen zu treffen.

Die Datenstrategie bemerkt außerdem korrekt an, dass automatisierte Produktpersonalisierung und Preisdifferenzierung zum Nachteil und zur Beeinflussung der Kunden eingesetzt werden können. Auch diese Technologien können als algorithmenbasierte Entscheidungssysteme verstanden werden.

> Im Sinne einer Algorithmenkontrolle sollte die Bundesregierung auch in diesem Kontext verpflichtende Regeln für Nachvollziehbarkeit-by-Design einführen, damit Aufsichtsbehörden Entscheidungskriterien und -logiken solcher algorithmischen Systeme nachvollziehen können.

Beispielsweise sollten die Aufsichtsbehörden im Verdachtsfall ein System hinsichtlich Irreführungen oder Diskriminierungen überprüfen können. Zudem sollte die Bundesregierung Anbieter dazu verpflichten, transparent auszuweisen, wenn Preise an den einzelnen Verbraucher angepasst werden. Hierbei sollten Anbieter auch offenlegen müssen, welche Datenkategorien in die Berechnung personalisierter Preise einfließen. Außerdem sollten Verbraucher hierin explizit einwilligen müssen.[40]

3.10 Datenteilungspflicht

Es ist erfreulich, dass die Bundesregierung prüfen möchte, ob auf besonders datengetriebenen Märkten eine Verpflichtung zum Teilen von bestimmten Daten erforderlich ist. Dies ist besonders aus wettbewerblichen Gründen zu begrüßen. Die jüngste Reform des Gesetzes gegen Wettbewerbsbeschränkungen[41] rückt Datenteilungspflichten stärker in den Fokus der Wettbewerbspolitik.

> Dementsprechend muss eine „Pflicht zur Datenteilung" so gestaltet werden, dass Wettbewerbsvorteile und Marktmacht großer datenverarbeitender Unternehmen und Plattformen gegenüber kleinen und mittleren Unternehmen nicht weiter verstärkt werden. Die Gestaltung von Maßnahmen zur Erleichterung des Datenzugangs für Unternehmen muss jedoch unter der Prämisse erfolgen, dass sie nicht zu einer Aufweichung des Datenschutzes führen und bei einem möglichen Zugriff auf personenbezogene Daten alle datenschutzrechtlichen Vorgaben zwingend beachtet werden.[42]

---

[40] Siehe auch Verbraucherzentrale Bundesverband: Personalisierte Preise (2016), URL: https://www.vzbv.de/meldung/ein-produkt-viele-preise [Zugriff: 17.02.2021].

[41] Vgl. Bundesregierung: Gesetz gegen Wettbewerbsbeschränkungen und für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz) (2021), URL: https://www.bundesregierung.de/breg-de/aktuelles/wettbewerbsrecht-1783534 [Zugriff: 01.02.2021].

[42] Vgl. European Data Protection Supervisor: Opinion 2/2021 on the Proposal for a Digital Markets Act (2021), S. 11f, URL: https://edps.europa.eu/sites/edp/files/publication/21-02-10-opinion_on_digital_markets_act_en.pdf [Zugriff: 18.02.2021]. Siehe auch Verbraucherzentrale Bundesverband: Fairen Wettbewerb in digitalen Märkten sicherstellen (2020), URL: https://www.vzbv.de/dokument/fairen-wettbewerb-digitalen-maerkten-sicherstellen [Zugriff: 17.02.2021].

Auch vor diesem Hintergrund begrüßt der vzbv, dass die Bundesregierung den Entwurf der Europäischen Kommission für einen Digital Markets Act (DMA) unterstützt. Dieser Rechtsakt wäre geeignet, eine Verpflichtung zum Teilen von bestimmten Daten europaweit zu verankern.

> Die Bundesregierung sollte im weiteren Gesetzgebungsprozess zum DMA außerdem darauf hinwirken, dass die vorgeschlagenen Verpflichtungen für Gatekeeper-Plattformen nicht abgeschwächt werden.

4. DATENKOMPETENZ

Der vzbv begrüßt, dass in der Datenstrategie der Kompetenzerwerb im Umgang mit Daten durch vielfältige Maßnahmen auf unterschiedlichen Ebenen hervorgehoben wird. Ebenso ist es begrüßenswert, dass Evidenzen zu Datenkompetenzen der Bevölkerung erhoben werden, um durch langfristiges Monitoring nationale und internationale Veränderungen zu erkennen und Ansätze zu identifizieren, mit denen Kompetenzerwerb gut funktioniert.

Auch sind die in der Strategie genannten Forschungsvorhaben ein wichtiger Baustein. Leider sind die verschiedenen Forschungsansätze nicht miteinander verknüpft und wenig konkret ausformuliert, so dass der konkrete Nutzen nicht hinreichend bewertet werden kann.

Bereits jetzt gibt es zahlreiche Bildungsplattformen auf Bundes- und Länderebene, die im Zuge der Corona-Pandemie verstärkt genutzt werden, die ausgebaut und leistungsfähiger gestaltet werden sollten. Dabei ist auf eine Interoperabilität der Angebote zu achten, um einen Austausch zu gewährleisten und die Entwicklung von einheitlichen Standards und Kriterien zu unterstützen. Ansätze wie bspw. Sodix, mit deren Hilfe die unterschiedlichen Systeme und Angebote der Länder miteinander vernetzt werden, sind hilfreich.

Auf der Ebene der Lern- und Materialangebote existieren bereits zahlreiche Materialdatenbanken, die Inhalte aufbereiten und detailliert auf ihre Qualität prüfen. Sie sind somit etablierte und vertrauenswürdige Partner für Lehrerinnen und Lehrer und für Schulen. In diesem Zusammenhang sind neue Materialdatenbanken, die die bereits vorhandenen Doppelstrukturen intensivieren, nicht hilfreich. Vielmehr sollten die bestehenden Angebote ausgebaut werden. Sinnvoll ist zudem eine intensivierte Zusammenarbeit der Materialdatenbanken, die sich in ihren unterschiedlichen Prüfansätzen sinnvoll ergänzen können.

> Eine bundesweite Bildungsplattform muss von unabhängiger Seite allerdings kritisch begleitet werden, um Interoperabilität zu bestehenden Angeboten zu gewährleisten und Qualitätskriterien für Methoden und Lernangebote und -inhalte zu etablieren, die einen Unterricht frei von wirtschaftlichen Interessen gewährleisten können. Auf der

> Ebene der Prüfung und Verfügbarmachung von Unterrichtmaterialien sollten die Erkenntnisse des Materialkompasses des vzbv berücksichtigt werden.[43]

Das geplante digitale Lernangebot zu „Datenkompetenz für alle“ muss sich zwingend im Bereich Schule entlang der Strategie der Kultusministerkonferenz Bildung für eine digitale Welt und den dort formulierten Kompetenzfeldern orientieren. Dabei sind kritische Reflexion der eigenen Datennutzung, sowie der eigenen Datensicherheitsmaßnahmen zu berücksichtigen. Das Lernen mit digitalen Medien ist wichtig, aber ebenso das Lernen über digitale Medien und den digitalen Lebensalltag - mit allen verbundenen Chancen und Risiken.

Um das IT-Sicherheitsniveau der Verbraucher zu erhöhen, ist die Verbesserung der IT-Sicherheitskompetenzen ein wichtiger Baustein. Für Verbraucher ist es beispielsweise aufgrund der mangelnden Datensicherheit bei vielen Anbietern wichtig, über grundlegende Datensicherheitskenntnisse zu verfügen. Beispielsweise sollten sie wissen, dass sie unterschiedliche Passwörter bei unterschiedlichen Diensten verwenden sollten und für die Anforderungen an ein sicheres Passwort sensibilisiert werden.

Zu Recht erwarten allerdings die meisten Verbraucher einen aktuellen und standardmäßigen Schutz für ihre Geräte und Anwendungen vor unberechtigtem Zugriff.[44] Denn mit individuellen Datensicherheitsmaßnahmen kommen Verbraucher sehr schnell an ihre Grenzen. Es wäre daher – um bei dem Beispiel zu bleiben – zu kurz gesprungen, lediglich von den Nutzern individuelle Maßnahmen, wie bessere Passwörter, zu erwarten. Die Verantwortung für die IT-Sicherheit darf nicht allein auf die Verbraucher abgewälzt werden.

> Vielmehr sind auch die datenverarbeitenden Stellen und Hersteller von Produkten gefragt, Datenschutz, Datensicherheit und IT-Sicherheit durch Technikgestaltung sicherzustellen. Hier bedarf es – wie oben angeführt – regulatorischer Anpassungen und der Einführung von verpflichtenden Mindestanforderungen an die sichere Gestaltung von Produkten und Anwendungen.

5. STAAT ALS VORREITER

Um den Staat als Vorreiter und Treiber einer verstärkten Datennutzung und Datenbereitstellung zu etablieren, sollte ein starker Fokus auf die Offenheit von Systemen und Informationen gelegt werden. Dementsprechend wird auch an mehreren Stellen der Datenstrategie Open-Source-Software eine Schlüsselrolle zugeschrieben. Daher ist es bedauerlich, dass die Bundesregierung keine konkreten Maßnahmen zur Förderung von Open-Source-Software in Erwägung zieht.

> Die Bundesregierung sollte daher offene Standards und Software fördern, beispielsweise indem diese Aspekte künftig bei Vergaben der öffentlichen Hand als Vergabekriterium aufgenommen werden. Darüber hinaus sollte öffentlich finanzierte Software

[43] Siehe auch Verbraucherzentrale Bundesverband (vzbv): Materialkompass - Das Schulportal für Verbraucherbildung, URL: https://www.verbraucherbildung.de/suche/materialkompass [Zugriff: 18.02.2021].

[44] Siehe auch Verbraucherzentrale Bundesverband (vzbv): Verbraucher setzen IT-Sicherheit voraus (2020), URL: https://www.vzbv.de/pressemitteilung/verbraucher-setzen-it-sicherheit-voraus [Zugriff: 18.02.2021].

> grundsätzlich auch der Allgemeinheit zur Verfügung gestellt werden („Public Money, Public Code“).

Darüber hinaus sollten Unternehmen, die im Auftrag öffentlicher Stellen beispielsweise im Rahmen der Stadtentwicklung tätig werden, verpflichtet werden, ihre in diesem Kontext verarbeiteten Daten dem Gemeinwohl zukommen zu lassen (Barcelona-Modell). So sollte beispielsweise auch ausgeschlossen werden, dass urheberrechtliche Erwägungen der Veröffentlichung von öffentlich finanzierten Gutachten und Studien entgegenstehen, um die daraus gewonnenen Erkenntnisse und Daten im Dienste der Gesellschaft verwenden zu können. Dies würde Marktmacht verringern und Innovation fördern.