

## Selbstbestimmter Umgang mit Daten

Wir alle erzeugen Daten, wir speichern und nutzen sie. Wir tun dies aus persönlichen, gesellschaftlichen, politischen, wissenschaftlichen oder wirtschaftlichen Gründen. Im digitalen Zeitalter verschwimmen dabei Grenzen. Die Masse an Daten wächst rasant. Und trotz ihrer Masse haften Daten an jedem Menschen, an jeder Maschine, an jedem Ort. Und schon wenige Daten lassen Rückschlüsse auf die Persönlichkeit und auf Nutzungs- und Aufenthaltsgewohnheiten zu. Als freie und demokratische Gesellschaft müssen wir klären, wie wir damit umgehen.

Als Jugendverbände stehen wir für Selbstbestimmung, gesellschaftliche Solidarität und soziale Gerechtigkeit. Diese Werte wollen wir in einer digitalen Gesellschaft zum Maßstab machen. Wir brauchen eine klare Haltung und verbindliche Regeln zwischen allen, die Daten bereitstellen, speichern, verwenden und auswerten – konkret zwischen Bürger\_innen, der Datenwirtschaft und dem Staat. Parallel zu konkrete Themen wie Datenschutz, Datensicherheit und Persönlichkeitsrechten müssen wir unsere Vorstellung einer digitalen Gesellschaft diskutieren.

Es ist nicht mehr möglich, keine Datenspuren zu hinterlassen. Deswegen müssen wir miteinander klären, wie Selbstbestimmung erhalten bleibt, wie ein sozialer, gerechter und rechtlicher Rahmen zur Nutzung persönlicher und öffentlicher Daten verbindlich geschaffen wird – über nationale Grenzen hinweg.

### *Recht auf informationelle Selbstbestimmung*

Das Recht auf informationelle Selbstbestimmung gehört zu den durch das Grundgesetz der Bundesrepublik Deutschland garantierten Grundrechten.<sup>1</sup> Das Bundesverfassungsgericht hat im Jahr 1983 klargestellt, dass jede\_r Bürger\_in das Recht hat, zu wissen, „wer was wann und bei welcher Gelegenheit über sie weiß“.<sup>2</sup> Die grundgesetzlich geschützte freie Persönlichkeitsentfaltung setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz der\_des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe ihrer\_seiner persönlichen Daten voraus.<sup>3</sup> Auch nach dem Recht der Europäischen Union hat jede Person das Recht auf den Schutz der sie betreffenden personenbezogenen Daten.<sup>4</sup> Im digitalen Zeitalter, in dem unvorstellbar viele Daten in der Welt verteilt auf Servern gespeichert sind und durch Algorithmen der Datenwirtschaft oder des Staates ausgewertet werden, läuft dieses Recht praktisch leer.

Informations- und Kommunikationstechnologie in Form von Geräten, Anwendungen und Plattformen sind heute immer zweierlei: Infrastruktur für soziales Handeln und Infrastruktur für die Erhebung von Daten über Menschen als handelnde Subjekte. Diese Informationen werden staatlich und kommerziell dazu genutzt, um das Handeln von Nutzer\_innen, Konsument\_innen und Bürger\_innen innerhalb und außerhalb der Infrastrukturen zu beeinflussen: Wer welche Inhalte und Suchergebnisse zu sehen bekommt, wer von Unternehmen wie behandelt wird und welche kommerziellen Privilegien (nicht) erhält, wer von staatlichen Behörden in seiner Privatsphäre und der Ausübung seiner Rechte eingeschränkt wird, wird durch diese Informationen beeinflusst.

Über jede\_n Einzelne\_n werden Unmengen von persönlichen Daten aus allen Lebensbereichen gespeichert, verarbeitet und genutzt. Es ist nicht mehr möglich, sich der massenhaften Speicherung von persönlichen Daten zu entziehen, weil – wo überhaupt eine Wahlmöglichkeit besteht – eine Ablehnung der Datenverarbeitung meist mit unmittelbaren persönlichen Nachteilen verbunden wird. Die bis heute weitgehend unregulierte Entwicklung und Ausbreitung der globalen Informationsindustrie verschärft das asymmetrische Machtgefüge zwischen Daten sammelnden und verwertenden Unternehmen auf der einen Seite sowie Nutzer\_innen, Konsument\_innen und Bürger\_innen auf der anderen Seite. Im Zentrum der Geschäftsmodelle dieser Industrie stehen algorithmische Systeme, die auf Grundlage der gesammelten Daten Prognosen über Menschen erzeugen und ihr Verhalten voraussagen und bewerten.

Herausgeber:  
Deutscher Bundesjugendring  
Mühlendamm 3, 10178 Berlin  
info@dbjr.de  
www.dbjr.de

gefördert durch:  
Bundesministerium für  
Familie, Senioren,  
Frauen und Jugend

Automatisierte Auswertung von Datenmassen stellt den Grundsatz der informationellen Selbstbestimmung in Frage. Wenn nicht jede\_r informiert ist und selbst entscheiden kann, welche persönlichen Informationen wem, wann und unter welchen Umständen und Fragestellungen zur Verfügung stehen können, dann wird schnell Wirklichkeit, auch über Wesentliches in unserer Gesellschaft nicht mehr frei entscheiden zu können. Weil die Lebenswelt von jungen Menschen von Informations- und Kommunikationstechnologie durchdrungen wird, werden über uns besonders viele Informationen gesammelt. Als Deutscher Bundesjugendring treten wir deswegen entschieden für die Verteidigung des digitalen Selbstbestimmungsrechts ein.

- ▶ *Wir fordern eine Wiederbelebung des Rechts auf informationelle Selbstbestimmung. Konkret fordern wir verbindliche, gerechte und soziale Rahmenbedingungen für die Nutzung persönlicher und öffentlicher Daten, die rechtlich verbindlich und durchsetzbar sind – über nationale Grenzen hinweg.*

### *Wirkungsvolle ePrivacy-Richtlinie*

In Europa ist mit der EU-Datenschutzverordnung<sup>5</sup> ein erster wichtiger Standard geschaffen worden – gegen heftige Widerstände internationaler Konzerne, die mit dem Datensammeln und -auswerten Handel treiben. Nun muss der nächste Schritt folgen, er steht mit der Reform der ePrivacy-Richtlinie an.

- ▶ *Wir fordern: Alle Institutionen der Europäischen Union müssen sicherstellen, dass der Schutz von Vertraulichkeit und Privatsphäre im Bereich elektronischer Kommunikation garantiert und modernisiert wird. Lücken, die die Datenschutzgrundverordnung noch lässt, müssen im Sinne eines umfassenden Verbraucherschutzes geschlossen werden. Dazu gehört auch eine Ausweitung des Geltungsbereichs der ePrivacy-Regeln auf Dienste wie Messenger, Internettelefonie, Webmail und Direktnachrichten in Sozialen Netzwerken.*

Wenn die einzige Alternative zur Einwilligung in die Erhebung und Verarbeitung personenbezogener Daten ist, von einem Angebot ausgeschlossen zu sein, kann nicht von einer freiwilligen Einwilligung ausgegangen werden.

- ▶ *Wir fordern, das Prinzip der informierten Einwilligung bei Erhebung und Verwertung personenbezogener Daten als Grundkonzept der reformierten ePrivacy-Richtlinie konsequent umzusetzen. Wir müssen in der Lage sein, bei der Einwilligung zur Erhebung und Verwertung unserer personenbezogenen Daten abzusehen, welche konkreten Prozesse der Verknüpfung, Analyse und Anwendung der Informationen zu erwarten sind - und welche Konsequenzen dies für unser Leben, insbesondere für unseren soziale und ökonomische Chancen hat.*

Sofern das nicht gegeben ist, kann ebenfalls nicht von einer freiwilligen Einwilligung ausgegangen werden. In der Konsequenz dürfen entsprechende Daten nicht gesammelt und verwertet werden. Jede\_r will schließlich nachvollziehen, welche Interessen und Muster hinter den Algorithmen stecken. Gerade weil die Essenz der Analyse großer Datenmengen Muster, Modelle, Aussagen und Hypothesen sind, die politische Entscheidungen prägen und auf das Leben großen Einfluss haben.

### *Anlasslose staatliche Massenüberwachung*

Nach der Rechtsprechung des Bundesverfassungsgerichts enthält das Recht auf informationelle Selbstbestimmung einen Schutzauftrag des Staates für seine Bürger\_innen: Der Staat muss jede\_n einzelne\_n Bürger\_in vor Übergriffen Dritter bewahren und durch das Ergreifen geeigneter Maßnahmen Rechtsgutsverletzungen verhindern.<sup>6</sup> Viel zu oft ist es aber der Staat, der in die digitale Privatsphäre eindringt. Meist mit Argumenten zur öffentlichen Sicherheit und Ordnung begründet, unternimmt der Staat viel, um persönliche Daten zu bekommen und auszuwerten. Beispiele hierfür sind die Vorratsdatenspeicherung, die Videoüberwachung im öffentlichen Raum oder das Terrorismusbekämpfungsgesetz. Stets erweiterte der Bundestag die Auskunftsbefugnisse und Datenzugriffe der Polizei, der Verfassungsschutzbehörden oder Nachrichtendienste. In staatlich organisierten Registern, wie beispielsweise dem Bundeszentralregister oder dem Ausländerzentralregister, werden ebenfalls persönliche Daten gespeichert und ausgewertet – alles unter mehr oder weniger strengen gesetzlichen Regeln. Trotzdem entfernen sich diese Gesetze immer mehr vom Grundsatz der Datensparsamkeit, der als Norm immer noch gilt. Abhilfe aus Karlsruhe ist kaum zu erwarten: Auch das Bundesverfassungsgericht verabschiedet sich mit seiner Rechtsprechung längst von den 1983 gesetzten Maßstäben.

- ▶ *Wir fordern ein Ende anlassloser und massenhafter staatlicher Datensammlungen! Wir fordern klare Regeln und Gesetze, die unser Recht auf informationelle Selbstbestimmung sichern und durchsetzen, eine staatliche und wirtschaftliche Auswertung in die Schranken weist und eine effektive parlamentarische Kontrolle der Geheimdienste gewährleistet. Die bestehenden Regeln zur Verarbeitung personenbezogener Daten durch öffentliche Stellen müssen entschieden verschärft werden und durch umfassendere Auskunft- und Löschanträge ergänzt werden.*

## Demokratie und private Räume

Demokratie braucht private Räume für die Meinungsbildung und öffentliche Räume für den gesamtgesellschaftlichen Diskurs. Mit zunehmender Überwachung werden die Grenzen der Privatheit aber verwischt, Vorhersagen von Handlungen aufgrund von Datenauswertung setzen uns in Abhängigkeit von Software, deren Kriterien und Rahmenbedingungen zur Zeit nicht von uns mitgestaltet werden können. Beide Aspekte können massiv einschränkend und reduktiv auf die Persönlichkeitsentwicklung junger Menschen wirken.

- ▶ *Wir fordern: Das Bedürfnis nach Sicherheit darf nicht zu einer Ausweitung datenerhebender Maßnahmen führen, sondern muss im demokratisch offenen Diskurs gesichert werden.*

Für junge Menschen spielt der staatliche Umgang mit dem Recht auf informationelle Selbstbestimmung im digitalen Alltag eine wesentliche Rolle. Junge Menschen bewegen sich jedoch vor allem in kommerziellen sozialen Netzwerken, nutzen Apps, spielen online und tragen Wearables, die pausenlos Daten erfassen, auf Server übertragen und auswerten. Ein Name ist für Algorithmen und jene, die deren Ergebnisse nutzen, am Ende gleichgültig, wenn Vorlieben, soziales Umfeld, Kaufkraft, Einstellungen, Orientierungen, Gesundheitszustand, Hobbies, Ausbildungs- und Arbeitsplätze, also (fast) alles bekannt ist.

## Privacy by Default und Privacy by Design

Eine Möglichkeit, sein Recht wahrnehmen zu können, ist Privacy by Default. Das heißt: Der Schutz der Privatsphäre, also der informationellen Selbstbestimmung, wird bereits in den Voreinstellungen im Sinne der Nutzer\_innen festgelegt. Bisher ist das Gegenteil die Regel: Allgemeine Geschäftsbedingungen und Datenschutzerklärungen sind lang, unverständlich, intransparent und in vielen Fällen ein Freibrief für die Anbietenden, mit den Daten alles zu machen. Niemand liest wirklich lange, hochkomplexe und unverständliche Klauseln und Paragraphen. Da eine Nutzung ohne eine „Zustimmung“ zu diesen Bedingungen in der Regel gar nicht möglich ist, erklären viele viel zu oft viel zu schnell das Einverständnis – häufig ohne genau zu wissen, in was sie eigentlich einwilligen.

- ▶ *Wir fordern eine konsequente Umsetzung des Privacy-by-Default-Prinzips bei der Gestaltung von Informations- und Kommunikationstechnologien. Wir fordern bei Datenschutzerklärungen und Geschäftsbedingungen eine klare, einfache Sprache. Grundeinstellung jedes Systems muss die datensparsame Option sein.*

Und selbst wenn junge Menschen sich bewusst entscheiden, welche Privacy-Option sie anklicken und was sie ins Netz stellen, ist das nur die offensichtlichste, aber lange nicht die wichtigste Quelle aus der die Datenkonzerne ihre Informationen beziehen, nutzen oder weiterverkaufen. Informations- und Kommunikationstechnologie ist voller Sensoren und Module für das Sammeln von Informationen. Entsprechend des Privacy-by-Design-Prinzips<sup>7</sup> sollte der Schutz der Privatsphäre deshalb schon in der Konzeption und Realisierung von Geräten, Anwendungen und Plattformen als oberste Maxime mitgedacht werden. Informationen, die für den eigentlichen Gebrauchszweck nicht wirklich notwendig sind, sollten gar nicht erst erhoben werden.

- ▶ *Wir fordern eine konsequente Umsetzung des Privacy-by-Design-Prinzips in der Gestaltung von Informations- und Kommunikationstechnologie. Technische Geräte sollten so gestaltet sein, dass möglichst wenig personenbezogene Daten anfallen.*

## Recht auf Einblick und Löschung

Junge Menschen sind vor der Auswertung ihrer Daten – und das heißt an dieser Stelle ihres Lebens – besonders zu schützen. Weil die Lebensphase Jugend sich auszeichnen muss durch freie Persönlichkeitsentfaltung, durch Freiräume von Konsequenzen und Verzweckung.

Letztlich Alle müssen die Möglichkeit zur Intervention haben, denn scheinbar überflüssige Informationen können wichtige Informationen werden: zum Beispiel für Arbeitgeber\_innen, Versicherungen oder Vertragspartner\_innen. Datenverarbeitende Unternehmen und Organisationen müssen einem Individuum gegenüber jederzeit in der Lage sein, verständliche, übersichtliche und umfassende Kenntnis der Informationen zu geben, die über eine\_n gespeichert sind.

Das Löschen der abgegebenen Daten bringt alle der informationeller Selbstbestimmung näher. Entscheidend wird sein, wie ein Rechtsstaat und die Europäische Union mit der EU-Datenschutzverordnung dies gegenüber den global agierenden Konzernen durchsetzt, die zum Beispiel nach US-amerikanischem Recht handeln. Im Rahmen der Privacy-Shield-Verabredung der EU-Kommission mit der US-Regierung sind bereits neue Auskunftsmechanismen für uns als Europäische Bürger\_innen gegenüber US-amerikanischen Firmen geschaffen worden. Das reicht nicht.

- ▶ *Wir fordern bereits jetzt eine konsequente Umsetzung des in der bald in Kraft tretenden EU-Datenschutzgrundverordnung festgeschriebenen „Rechts auf Löschung“. Alle müssen die Möglichkeit haben, die über sie bei einer Organisation gespeicherten personenbezogenen Daten standardisiert und simpel löschen lassen zu können, ohne dass daraus soziale oder ökonomische Nachteile entstehen.*

## Soziale Gerechtigkeit vor persönlichem Komfort

Wenn es um einen Verwendungszweck geht, der das Leben erleichtert und vielleicht sogar auf den ersten Blick der Allgemeinheit dienen könnte, stellen viele vielleicht bereitwilliger Daten zur Verfügung. Ein paar Beispiele: Diagnostik in der Medizin kann durch die Auswertung von Daten aus Fitnessuhren verbessert werden, Energiebedarfe lassen sich bereits exakt durch ein Netz aus Sensoren steuern, Abfahrtszeiten im Öffentlichen Personennahverkehr werden in Echtzeit im Mobilgerät angezeigt...

Kommerzielle Angebote, die aufgrund persönlicher Daten und deren Auswertung maßgeschneidert und für jede\_n persönlich günstig erscheinen, gibt es inzwischen sehr viele. Krankenkassen bieten etwa spezielle Tarife für alle, die ihre Gesundheitsdaten permanent auswerten lassen. Oder Autoversicherungen rechnen nach dem individuell aufgezeichneten Fahrverhalten ab. Das klingt komfortabel und günstig, hat aber auch eine Kehrseite: Unternehmen streichen aufgrund der BigData-Analysen Leistungen, Versicherungen verweigern den Schutz. Persönlicher Vorteil geht insgesamt zu Lasten einer solidarischen und gerechten Gesellschaft.

- ▶ *Wir fordern, dass personenbezogene Daten nicht für ein „social profiling“ oder „racial profiling“ genutzt werden dürfen. Die Erhebung und Verwertung dieser Daten darf keine neuen sozialen Ungleichheiten produzieren.*
- ▶ *Wir fordern, dass personenbezogene Daten, die eindeutig Minderjährigen zuzuordnen sind, nicht kommerziell erhoben und verwertet werden dürfen. Für die wissenschaftliche Nutzung müssen diese Daten soweit anonymisiert sein, dass ein Rückschluss auf einzelne Kinder und Jugendliche nicht möglich ist.*

## Was wir tun müssen

Als Jugendverbände und -ringe müssen wir dafür einstehen und kämpfen, dass auch in einer digitalen Gesellschaft eine Politik gemacht wird, die das Soziale in den Mittelpunkt stellt. Und wir müssen uns dagegen verwahren, dass eine Mischung aus neoliberaler Haltung (alle müssen selbst für den Datenschutz sorgen) mit einer opportunistischen Politik (der Staat darf selbst alle Daten nutzen, um zu kontrollieren) vorherrscht.

Unsere Ansprüche und unsere Forderungen bedeuten, unser eigenes Handeln in den Jugendverbänden und Jugendringen kritisch zu reflektieren und digitale Umgebungen zu nutzen bzw. zu empfehlen, die unseren Grundwerten entsprechen: Zum Beispiel Dezentrale Netzwerke wie Freifunk oder Cloudlösungen, die Datenschutz realisieren, wie wir ihn verstehen.

Wir müssen uns fragen, wie wir mit Daten umgehen, wie wir das Recht auf informationelle Selbstbestimmung sichern, Privacy by Default und Privacy by Design bei unseren Angeboten sicherstellen, dem Grundsatz der Datensparsamkeit folgen und das Recht auf Löschen umsetzen. Wir müssen klären, wie wir die Prozesse unserer Datenverarbeitung transparent machen und niemanden digital ausschließen. Wir müssen dazu unsere medienpädagogischen Angebote weiterentwickeln und uns für eine Stärkung emanzipatorischer Digitalbildung einsetzen. Und wir müssen medien- und netzpolitisch aktiver sein. Bestrebungen, Maßnahmen zur Vermittlung von Medienkompetenz vor allem im erzieherischen Kinder- und Jugendschutz zu verorten, lehnen wir entschieden ab.

#### Fussnoten

1. Das Recht auf informationelle Selbstbestimmung ist im bundesdeutschen Recht das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Es handelt sich dabei nach der Rechtsprechung des Bundesverfassungsgerichts um ein Datenschutz-Grundrecht, das im Grundgesetz für die Bundesrepublik Deutschland nicht ausdrücklich erwähnt wird. Der Vorschlag, ein Datenschutz-Grundrecht in das Grundgesetz einzufügen, fand bisher nicht die erforderliche Mehrheit.
2. Bundesverfassungsgericht, Urteil vom 15.12.1983, BVerfGE Bd. 65, Seite 1 (Volkszählung), Seite 43.
3. Bundesverfassungsgericht, ebenda.
4. Vgl. Charta der Grundrechte der Europäischen Union, 30.03.2010, Amtsblatt der Europäischen Union 2010 C 83/391, Artikel 8
5. Datenschutz ist ein in der zweiten Hälfte des 20. Jahrhunderts entstandener Begriff, der teilweise unterschiedlich definiert und interpretiert wird. Je nach Betrachtungsweise wird Datenschutz verstanden als Schutz vor missbräuchlicher Datenverarbeitung, Schutz des Rechts auf informationelle Selbstbestimmung, Schutz des Persönlichkeitsrechts bei der Datenverarbeitung und auch Schutz der Privatsphäre.
6. Der Schutzauftrag des Staates resultiert u.a. aus den europäischen Erfahrung von Diktatur und Kontrolle durch den Staat. Die Nationalsozialisten etwa haben Daten genutzt, um Juden und Andersdenkende zu verfolgen (und dazu akribisch Daten gesammelt). Basis für das Recht in Deutschland sind die Artikel 1 und 2 des Grundgesetzes.
7. „Privacy by Design“ bedeutet „Datenschutz durch Technik“ und soll sicherstellen, dass Datenschutz und Privatsphäre schon in der Entwicklung von Technik beachtet werden. Technik ist dann so angelegt, dass die Privatsphäre von Nutzer:innen geschützt wird und, dass Anwender:innen Kontrolle über die eigenen Informationen haben. Außerdem will „Privacy by Design“ für Organisationen auch für einen Wettbewerbsvorteil gegenüber Konkurrenten sorgen. Dahinter steht die Überlegung, dass Nutzer:innen sich im Zweifel für datenschutzfreundliche Produkte entscheiden. (<https://digitalcourage.de/blog/2015/was-ist-privacy-design>)

*Mehrheitlich bei drei Nein-Stimmen\* und vier Enthaltungen beschlossen auf der 89. Vollversammlung am 28./29. Oktober 2016 in Berlin.*

*\*Die Deutsche Beamtenbundjugend erklärt mit Verweis auf §14, Absatz 2 der DBJR-Satzung, dass der Beschluss gegen ihre Grundsätze verstößt.*