„BIG DATA UND DATENSCHUTZ“

Big Data Analysen können ein gewaltiger Gewinn für einzelne Verbraucherinnen und Verbraucher sein und zur Lösung gesellschaftlicher Probleme beitragen: Das digitale Auto beispielsweise ist mit der Infrastruktur und anderen Fahrzeugen vernetzt, um einen Stau rechtzeitig zu erkennen, Verkehrsinformationen zu beziehen oder Unfälle zu melden. Es erkennt seine Fahrer und richtet die Einstellungen des Innenraums oder das Entertainmentprogramm nach deren individuellen Vorlieben ein. Das ist nicht nur bequem, sondern kann gleichzeitig die Sicherheit erhöhen und die Umwelt entlasten. Und auch in der Medizin kann mit Big Data Technologien den Patienten geholfen und Kosten gesenkt werden. Beispielsweise lassen sich Krebserkrankungen leichter analysieren und erforschen. Auf dieser Basis können anschließend individuelle Behandlungstherapien entwickelt werden.

Big Data birgt aber auch genauso gewaltige Gefahren für Verbraucherinnen und Verbraucher: Je mehr eine Person, ein Unternehmen oder ein Staat über uns weiß, umso einfacher ist es für sie, uns zu manipulieren und zu kontrollieren. Darum muss der Einzelne grundsätzlich selbst darüber entscheiden können, welche Daten er preisgibt und wie diese Daten verwendet werden dürfen. Zur persönlichen Freiheit gehört es, Dinge zu tun und zu lassen, ohne dass andere davon wissen. Diese Freiheit wurde in den vergangenen Jahren immer stärker ausgehöhlt. Vorlieben, Ansichten und Verhaltensweisen werden systematisch gesammelt und in Profilen zusammengefasst. Algorithmen entscheiden bereits heute nicht nur welche Werbung Nutzer im Internet sehen, sondern könnten auch bestimmen, welchen Preis sie individuell für ein Produkt zahlen oder welche Informationen sie auf Nachrichtenseiten oder durch Suchmaschinen erhalten – und die zukünftigen Risiken gehen weit darüber hinaus.

Nun darf aber nicht der Fehler begangen werden, Datenschutz und Big Data gegeneinander auszuspielen. Die Debatte darf nicht auf ein entweder/oder und somit auf ein Nullsummenspiel reduziert werden.

> Die Herausforderung lautet, die Chancen von Big Data zu nutzen, aber gleichzeitig die Risiken zu minimieren. Die bestehenden Grundsätze des Datenschutzes, die in der Europäischen Union Grundrechtscharakter haben, müssen dabei weiterhin Bestand haben: Zweckbindung, Datensparsamkeit und Einwilligungsvorbehalt.

Gleichzeitig muss klar sein, dass ein – begründetes – Vertrauen der Verbraucher mittelfristig eine Grundvoraussetzung für den Erfolg von Big Data und entsprechenden datenintensiven Geschäftsmodellen ist. In einer breit angelegten Umfrage des Vodafone Instituts für Gesellschaft und Kommunikation vom Januar 2016 spiegelt sich das – oftmals zu Recht – geringe Vertrauen der Verbraucherinnen und Verbraucher in datenverarbeitende Dienste wieder. Beispielsweise vermeiden es 56 Prozent der deutschen Befragten, sehr persönliche Dinge in E-Mails oder Textnachrichten zu schreiben, da sie

befürchten, dass Dritte darauf zugreifen könnten[1]. Und selbst wenn ihre Daten anonymisiert wären, würden sich nur 42 Prozent der Befragten noch wohl damit fühlen, diese Daten an die Gesundheitsforschung zu geben[2]. Dies zeigt, dass sogar die Erfolgschancen vorbildlicher oder datenschutzfreundlicher Dienste durch das geschwundene Vertrauen der Verbraucher in Mitleidenschaft gezogen werden können. Im Gegensatz dazu wirkt richtig verstandener und gut umgesetzter Datenschutz vertrauensbildend. So gab die Mehrzahl der Befragten an, dass klare und einfache Darstellung von Datenschutzbestimmungen (76 Prozent) sowie die transparente Darstellung der Verarbeitungszwecke (57 Prozent) ihr Vertrauen in datenverarbeitende Unternehmen stärken würde[3].

> Der verantwortungsvolle Umgang mit den Daten der Nutzer, Offenheit und Transparenz bei der Verarbeitung personenbezogener Daten müssen die oberste Maxime bei der Anwendung von Big Data und die Entwicklung datenintensiver Geschäftsmodelle sein. Nutzer dürfen sich den Prozessen nicht schutzlos ausgesetzt fühlen. Sie müssen mitbestimmen können, ob und in welcher Form ihre Daten verarbeitet und analysiert werden und die Konsequenzen nachvollziehen können. Somit kann das Risiko von negativen Auswirkungen der Datenverarbeitung, wie Manipulation, Diskriminierung und Fremdbestimmung verringert werden.

Der Schutz von persönlichen Daten von Verbrauchern und das Recht auf Privatsphäre kann die Konsequenz nach sich ziehen, dass nicht jedes beliebige Geschäftsmodell realisiert werden kann. Doch wer dabei laut aufschreit, sollte sich dabei genau überlegen, ob es ratsam ist Geschäftsmodelle zulassen, bei denen die Verarbeitung von persönlichen Daten und ihre Zwecke nicht mehr kontrollierbar und Entscheidungen nicht mehr nachvollziehbar sind? Auf die Frage, wie der Einzelne und die Gesellschaft dann vor Kontrolle und Manipulation geschützt werden sollen, kann bisher keiner eine Antwort liefern, der vor einem zu starken Datenschutz warnt.

Kontakt

Verbraucherzentrale Bundesverband e.V.
Team Digitales und Medien
Markgrafenstraße 66, 10969 Berlin
digitales@vzbv.de

[1] Vodafone Institute for Society an Communications; Big Data – A European survey on the opportunities and risks of data analytics; Januar 2016, Seite 56 http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-en.pdf
[2] Ebenda; Seite 122
[3] Ebenda; Seite 48