Marit Hansen

Herausforderung Verbraucher-datenschutz in der digitalen Welt

gute gesellschaft –
soziale demokratie
#2017 plus

FRIEDRICH EBERT STIFTUNG

gute gesellschaft –
soziale demokratie
2017 plus

EIN PROJEKT DER FRIEDRICH-EBERT-STIFTUNG
IN DEN JAHREN 2015 BIS 2017

Was macht eine Gute Gesellschaft aus? Wir verstehen darunter soziale Gerechtigkeit, ökologische Nachhaltigkeit, eine innovative und erfolgreiche Wirtschaft und eine Demokratie, an der die Bürgerinnen und Bürger aktiv mitwirken. Diese Gesellschaft wird getragen von den Grundwerten der Freiheit, Gerechtigkeit und Solidarität.

Wir brauchen neue Ideen und Konzepte, um die Gute Gesellschaft nicht zur Utopie werden zu lassen. Deswegen entwickelt die Friedrich-Ebert-Stiftung konkrete Handlungsempfehlungen für die Politik der kommenden Jahre. Folgende Themenbereiche stehen dabei im Mittelpunkt:

- Debatte um Grundwerte: Freiheit, Gerechtigkeit und Solidarität;
- Demokratie und demokratische Teilhabe;
- Neues Wachstum und gestaltende Wirtschafts- und Finanzpolitik;
- Gute Arbeit und sozialer Fortschritt.

Eine Gute Gesellschaft entsteht nicht von selbst, sie muss kontinuierlich unter Mitwirkung von uns allen gestaltet werden. Für dieses Projekt nutzt die Friedrich-Ebert-Stiftung ihr weltweites Netzwerk, um die deutsche, europäische und internationale Perspektive miteinander zu verbinden. In zahlreichen Veröffentlichungen und Veranstaltungen in den Jahren 2015 bis 2017 wird sich die Stiftung dem Thema kontinuierlich widmen, um die Gute Gesellschaft zukunftsfähig zu machen.

Weitere Informationen zum Projekt erhalten Sie hier:
www.fes-2017plus.de

FRIEDRICH-EBERT-STIFTUNG

AUF EINEN BLICK

Die Bedeutung von Datenschutz für Verbraucher_innen wird wichtiger in dem Maße, in dem die digitale Welt in alle Lebensbereiche Einzug hält. Die Dominanz von wenigen marktbeherrschenden Unternehmen, Cloud Computing, Big Data und Sensorik stellen Herausforderungen an den Verbraucherdatenschutz: Systeme müssen datenschutzgerecht gestaltet werden, Transparenz und Intervenierbarkeit für die Betroffenen sind zu verbessern.

Die Informationsgesellschaft ist geprägt von einer zunehmenden Datenverarbeitung, die mittlerweile alle Lebensbereiche berührt oder sogar durchdringt. Verbraucher_innen sind gegenüber denjenigen Stellen, die Daten über sie sammeln und auswerten, in einer schwächeren Machtposition. Das Datenschutzrecht soll für Fairness bei der Verarbeitung von personenbezogenen Daten sorgen.

Grundlage des Datenschutzverständnisses in Deutschland ist das Recht auf informationelle Selbstbestimmung, das 1983 vom Bundesverfassungsgericht im sogenannten Volkszählungsurteil begründet wurde: Jede_r soll grundsätzlich selbst über die Preisgabe und Verwendung ihrer bzw. seiner personenbezogenen Daten bestimmen können. Dazu gehört auch zu wissen, wer was wann über einen weiß.

DAS KLEINE 1X1 DES DATENSCHUTZES

Verarbeitet eine Organisation personenbezogene Daten, so ist dies nach deutschem Datenschutzrecht nur erlaubt, wenn es dafür eine Rechtsgrundlage gibt oder wenn die Betroffenen eingewilligt haben. Voraussetzung für eine wirksame Einwilligung sind Freiwilligkeit und Informiertheit, d. h. die Betroffenen dürfen nicht zu einer Einwilligung gedrängt werden und sie müssen nachvollziehen können, worin sie einwilligen und welche Konsequenzen daraus resultieren. Sie können zudem ihre Einwilligung mit Wirkung für die Zukunft zurückziehen.

Der Zweck der Verarbeitung ist vorab zu definieren, d. h. für einen Zweck erhobene Daten dürfen nicht für beliebige Zwecke genutzt werden. Nur solche personenbezogenen Daten dürfen verarbeitet werden, die für den jeweiligen Zweck erforderlich sind. Transparenz über die Datenverarbeitung ist wichtig. Betroffene haben das Recht auf Auskunft zu ihren Daten, auf Korrektur fehlerhafter Daten und auf Löschung, wenn die Daten nicht oder nicht mehr verarbeitet werden dürfen. Natürlich muss eine datenverarbeitende Stelle die Daten und die Verarbeitungssysteme durch technische und organisatorische Maßnahmen gegen Missbrauch schützen.

Innerhalb der Europäischen Union (EU) sind diese Regelungen ähnlich ausgestaltet. Allerdings gibt es auch Länder, in denen personenbezogene Daten keinen derartigen rechtlichen Schutz genießen und wo Prinzipien wie der Zweckbindungsgrundsatz oder Überlegungen zur Erforderlichkeit nahezu unbekannt sind.

EIGENSCHAFTEN, TRENDS UND GEFAHREN UNSERER DIGITALEN WELT

Typisch für die digitale Welt ist die Transformation von Informationen in Formate, die beliebig kopierbar und auswertbar sind. Bei jeglicher Nutzung fallen normalerweise Datenspuren an. Datenbestände können über Netze hinweg miteinander in Beziehung gesetzt werden. Interessen, Konsum, Standorte, Meinungen, persönliche Eigenschaften – alles wird verkettbar. Big Data verspricht Analyse-Ergebnisse auch zu vorher unbekannten Korrelationen. Cloud Computing ermöglicht das bedarfsgerechte Verwenden von Ressourcen in Rechenzentren rund um den Globus mit Unterstützung diverser Dienstleister, deren Zugriff auf die Daten nicht ausgeschlossen werden kann. Smart Homes, Smart Cars und Smart Cities basieren auf einer Vielzahl von kleinen Sensoren, mit deren Hilfe die Umgebung ausgewertet werden kann. Gut für Energieeffizienz oder sicheres Autofahren, jedoch schlecht, wenn für einen staatlichen „Big Brother" oder für Firmen als „Smart Sisters" die Verbraucher_innen gläsern werden.

All dies passiert technikgestützt und automatisiert, das bedeutet: auf Basis von Maschinen, Infrastrukturen und Dienstleistern, deren Vertrauenswürdigkeit nicht gewährleistet ist. Weiterhin wird der Markt dominiert von relativ wenigen, aber sehr mächtigen Quasi-Monopolisten, die sich zentral an wichtigen Schaltstellen positioniert haben. So besteht eine Abhängigkeit von in China produzierter Hardware wie Computer-Chips; an US-amerikanischen Dienstleister kommen Verbraucher_innen kaum vorbei, wenn sie Smartphones haben oder Internet-Angebote nutzen möchten. Man hat sich daran gewöhnt, für Internet-Services kein Geld zahlen zu müssen – dass damit aber ein „Bezahlen" mit den eigenen Daten einhergeht, was so nicht mit deutschem Datenschutzrecht vereinbar ist, wird oft übersehen. Rechtskonforme Alternativen haben es daher häufig schwerer.

Big Data kann viele neue Möglichkeiten bieten für die Organisation des Alltags, für politische Teilhabe, für die persönliche Selbstentfaltung, für wirtschaftliche Wertschöpfung und die Lösung gesellschaftlicher Probleme. Die Gefahren, die aus einer schrankenlosen Datenpreisgabe und -analyse entstehen, sollten jedoch nicht unterschätzt werden. Bereits heute werden die gesammelten Verbraucherdaten für eine umfassende Profilbildung genutzt, im harmloseren Fall zur gezielten Platzierung von Werbung, im Zweifel aber zur Diskriminierung von Verbraucher_innen etwa über teurere Versicherungstarife oder schlechtere Kreditkonditionen. Die Preisgabe von Verbraucherdaten kann also erhebliche Auswirkungen haben. Es besteht letztlich die Gefahr, dass durch die zunehmende Digitalisierung aller Lebensbereiche Unternehmen (oder auch staatliche Stellen) in nie gekannter Weise Einblick in wesentliche Teile der Lebensgestaltung der Bürger_innen erhalten und dieses Wissen zum Nachteil der Bürger_innen oder Verbraucher_innen verwendet wird.

Zudem basiert Big Data meist auf vorhandenen oder billig zu bekommenden Daten. Es ist riskant, auf dieser Basis Entscheidungen zu treffen, weil der Datenbestand verzerrt sein kann: Beispielsweise darf eine Verkehrsplanung nicht allein auf gesammelten Bluetooth-Daten vorbeifahrender Autos beruhen, denn dann wären diejenigen in der Erhebung nicht repräsentiert, die keine Bluetooth-Geräte mit sich führen

oder Bluetooth z. B. aus Datenschutzgründen deaktiviert haben.

Die Entwicklung zu einer Gesellschaft, in der Personen mit Datenschutzbedarf diskriminiert werden, wäre hochproblematisch. Dies beginnt schon beim freiwilligen (?) Vorzeigen einer Schufa-Selbstauskunft als Mietinteressent_in: Wer nicht von Anfang an die Kreditwürdigkeit unter Beweis stellt, hat möglicherweise später keine Gelegenheit mehr dazu. Ähnliches kann sich bei Kommunikation der Fitnesswerte aus dem Trend der Selbstvermessung („Quantified Self") entwickeln: Wer gar nicht mitmacht oder aussetzt, muss vielleicht höhere Versicherungskosten zahlen oder hat schlechtere Einstellungschancen.

SCHÖNE GEWOHNHEITEN

Verbraucher_innen in Deutschland sind gewohnt, dass sie nie schutzlos dastehen, sondern vom Datenschutzrecht oder vom ausgefeilten Recht über die Allgemeinen Geschäftsbedingungen (AGB) geschützt werden. Aber die Realität ist anders: Gerade bei den vermeintlich kostenlosen Angeboten von global auftretenden Dienstleistern kann man einmal offenbarte Daten faktisch nicht mehr zurückholen. Speicherungen von Daten deutscher Verbraucher_innen in ausländischen Unternehmens- oder Geheimdienstdatenbanken – selbst wenn sie nach deutschem oder europäischem Recht unzulässig wären – sind in dieser Zeit auch für Aufsichtsbehörden nicht effektiv kontrollierbar.

Wenn die Absicherung mit Netz und doppeltem Boden im Daten- und Verbraucherschutzrecht nicht mehr funktioniert, könnte man meinen, dass die Verbraucher_innen einfach selbst mehr Verantwortung für ihre Daten übernehmen müssen. Für Internet-Dienste gibt es mittlerweile vielfältige Selbstdatenschutz-Tools: zur Verschlüsselung, zur Anonymisierung, zum Blockieren von Tracking-Funktionalität usw. Doch es ist eben nicht einfach, sich selbst zu schützen. Das liegt nicht nur an Problemen mit der Benutzbarkeit der Tools, sondern ohne die Kooperation der Datenverarbeiter wird es vielfach schwer, die Risiken für die Privatsphäre überhaupt zu verstehen geschweige denn eigene Maßnahmen dagegen zu ergreifen.

Kaum jemand macht sich z. B. bewusst, dass Multifunktionskopierer die kopierten Daten in der Regel auf Festplatte zwischenspeichern und diese durch Service-Personal oder manchmal sogar durch nachfolgende Kund_innen im Copyshop auslesbar sein können. Das neue Fernsehgerät (Smart-TV) leistet zwar mehr, wenn es mit dem Internet verbunden ist, jedoch ahnen die wenigsten, dass bei einigen Geräten USB-Speichermedien nicht nur lokal ausgelesen, sondern die Informationen über das Netz verschickt werden, oder dass Hersteller oder Fernsehsender Tracking-Funktionalität eingebaut haben, mit denen das Nutzerverhalten beobachtbar ist.

GANZ WICHTIG: TRANSPARENZ

Also lautet die Parole: verständliche Informationen an alle Verbraucher_innen! Leichter gesagt als getan, denn oft wissen die datenverarbeitenden Stellen selbst nicht, wie die von ihnen zu verantwortende, aber mit Hilfe anderer realisierte Datenverarbeitung funktioniert. Verwendet ein Unternehmen z. B. eine Facebook-Fanpage, müssten sowohl Facebook-Mitglieder als auch –Nichtmitglieder darüber aufgeklärt werden, was Facebook mit den Daten der Nutzer_innen macht. Diese Informationen liegen aber nicht vor, auch nicht in den ca. 70.000 Zeichen umfassenden Dokumenten mit Datenschutzbezug.[1]

Ohnehin führt ein reiner Verweis auf die oftmals vorhandenen, wenn auch nicht verständlichen Datenschutzerklärungen (Privacy Policies) in die Irre, denn welche Verbraucher_innen studieren ernsthaft solche Texte vor der Nutzung? Im deutschen AGB-Recht wird dies dadurch adressiert, dass Regelungen in den AGB, die nicht erwartungskonform sind oder die Verbraucher_innen unangemessen benachteiligen, unwirksam sind. Geht es allerdings um das Einholen einer datenschutzrechtlichen Einwilligung, müssen die Betroffenen informiert sein – sonst wäre die Einwilligung nicht gültig.[2]

Es gibt aber weitere Einschränkungen: Bei Mobiltelefonen ist das Mini-Display für lange Informationstexte ungeeignet. Und wie sollen Verbraucher_innen die Aktivität von Sensoren, die in einer Smart City allgegenwärtig im Raum untergebracht sein können, und die Auswertung der Daten nachvollziehen können?

Zwar wird schon seit Jahren an Lösungsvorschlägen gearbeitet, beispielsweise durch Mehrebenen-Policies, die mit einem kurzen Überblick beginnen und für Interessierte detailliertere Informationen bereithalten; durch Piktogramme, die aber standardisiert sein müssten; oder durch maschinell übertragene Policies, die vom eigenen Endgerät der Nutzer_innen interpretiert und mit den eigenen Anforderungen abgeglichen werden. Doch entwickeln sich die komplexen Geflechte der Datenverarbeitungssysteme schneller, als dass messbare Fortschritte im Verständlichmachen eingetreten wären. Hier fehlt es womöglich an einer Motivation der Datenverarbeiter: Was wäre, wenn alle Datenverarbeitung, die auf Einwilligung beruht, sofort stoppen müsste, sobald sich herausstellte, dass die Betroffenen gar nicht verstanden haben, auf was sie sich einlassen? Andererseits: Im AGB-Recht mutet man den Verbraucher_innen eben nicht zu, alles genau zu lesen.

EFFEKTIV EINGREIFEN KÖNNEN

Im internationalen Rahmen verspricht man sich seit Jahren viel vom Prinzip „Notice & Choice", also der Wahlmöglichkeit nach dem Informationshinweis. Allerdings ist dieses Prinzip kein Garant für Verbraucherdatenschutz. Zum einen ist die Umsetzung nicht ausreichend, da Transparenz über Art und Umfang der Datenverarbeitung oftmals nicht hergestellt ist.[3] Zum anderen greift „Choice" im Sinne der Auswahl zwischen wenigen vorgegebenen Alternativen zu kurz. Dies liegt nicht nur daran, dass Angebote mit einem hohen Datenschutzniveau oftmals gar nicht zur Auswahl stehen oder Verbraucher_innen bei der Wahl ausgetrickst werden können[4], sondern auch an einem Mangel an Möglichkeiten für ein effektives Intervenieren. Im Cloud Computing könnte es beispielsweise notwendig sein, personenbezogene Daten unmittelbar aus dem Zugriffsbereich nicht-vertrauenswürdiger Dienstleister

zu entfernen. In einem Smart Home müssen die Bewohner_innen die Sensoren ausschalten können, wenn ihnen danach ist. Zudem müssen die Betroffenen komfortabel ihre Rechte auf Auskunft, Korrektur, Löschung oder Widerspruch wahrnehmen können.

FREMDWIRKUNG VON SELBSTBESTIMMUNG

In unserer vernetzten Welt kann sich jede Entscheidung einer Person auch auf andere auswirken. Wer z. B. Telefonnummern ins Smartphone-Adressbuch einträgt, überträgt diese Daten über andere Personen damit in der Regel in die Cloud von Google, Apple o. ä. Mit dem Verwenden einer kostenlosen Gmail-Adresse geht einher, dass alle Nachrichten dorthin von Google inhaltlich gescannt werden. Welchen Absender_innen ist dies bewusst, bevor sie eine E-Mail an eine solche Adresse schicken? Wer seine Gendaten online stellt, verrät auch Informationen über seine Familie, selbst über noch nicht geborene Nachfahren.

FAZIT UND POLITISCHE HANDLUNGS-OPTIONEN

Voraussichtlich wird in Kürze die EU-Datenschutz-Grundverordnung beschlossen, mit der dieselbe Interpretation der Datenschutzregeln in allen Mitgliedstaaten erreicht werden soll. Darin sind insbesondere Prinzipien wie „Privacy by Design" (Datenschutz muss in die Systeme eingebaut sein) und „Privacy by Default" (datenschutzfreundliche Voreinstellungen) enthalten. Wird dies von Herstellern, datenverarbeitenden Stellen und Aufsichtsbehörden ernstgenommen, ist es eine gute Nachricht für den Verbraucherdatenschutz. Allerdings ist die implementierte und gelebte Realität zurzeit weit entfernt von dem technisch Möglichen für einen besseren Datenschutz. Es ist den meisten Akteuren gar nicht bekannt, welche Methoden bereits jetzt einsatzbereit sind oder in Kürze zur Verfügung stehen werden.[5] Für die Erarbeitung von Best-Practice-Lösungen, die allen als Orientierung dienen sollen, müssen Verbraucher- und Datenschützer_innen an einem Strang ziehen. Vertrauenswürdige Gütesiegel können auch im Datenschutzbereich Verbraucher_innen darin unterstützen, die guten Produkte zu erkennen, und für Unternehmen Marktanreize für eingebauten und gelebten Datenschutz schaffen.

Gleichzeitig ist die Politik gefragt, um das Datenschutzrecht weiterzuentwickeln zu einem übergreifenden Informationsrecht, das nicht nur Auswirkungen für den Einzelnen, sondern auch mögliche Effekte auf Gruppen im Blick hat, z. B. Zwänge, Fremdbestimmungen oder Diskriminierungen. Die Blaupause für einen zukunftsfähigen Masterplan, der die vielfältigen gesellschaftlichen Interessen berücksichtigt und zu einem fairen Ausgleich bringt, fehlt noch. Klar ist aber jetzt schon, dass es nicht ausreicht, sich auf Selbstregulierung zu verlassen, dass Verbraucherdatenschutz dringend in der technischen Standardisierung einbezogen und gestärkt werden muss, und dass Verbraucher- und Datenschützer_innen genügend Ressourcen und effektive Instrumente benötigen, um die Rechte der Menschen in der Informationsgesellschaft – oft gegen die Interessen kapitalstarker Unternehmen und überbordend kontrollierender Staaten – durchzusetzen.

Autorin

Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein, Kiel.

Anmerkungen

1 – Der Umfang ergibt sich aus Facebooks Dokumenten „Erklärung der Rechte und Pflichten" (https://de-de.facebook.com/legal/terms), „Datenrichtlinie" (https://de-de.facebook.com/about/privacy) sowie „Cookies, Pixel und ähnliche Technologien (https://de-de.facebook.com/help/cookies), abgerufen im Juli 2015. Daneben wären weitere Facebook-Informationen zu studieren.
2 – Kamp, Meike; Rost, Martin: Kritik an der Einwilligung, in: Datenschutz und Datensicherheit (DuD) 37, 2 (2013), S. 80–84.
3 – Federal Trade Commission: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, März 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (15.9.2015).
4 – Adjerid, Idris; Acquisti, Alessandro et al.: Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, in: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13), New York 2013, Article No. 9.
5 – Danezis, George; Domingo-Ferrer, Josep et al.: Privacy and Data Protection by Design – from policy to engineering, European Union Agency for Network and Information Security (ENISA), Dezember 2014, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design (15.9.2015).

Impressum

© 2015
Friedrich-Ebert-Stiftung
Herausgeber: Abteilung Wirtschafts- und Sozialpolitik
Godesberger Allee 149, 53175 Bonn
Fax 0228 883 9205, www.fes.de/wiso

Für diese Publikation ist in der FES verantwortlich:
Dr. Robert Philipps, Abteilung Wirtschafts- und Sozialpolitik
Bestellungen/Kontakt: wiso-news@fes.de
Titelmotiv: himberry / photocase.de

ISBN: 978-3-95861-281-5