Peter Schaar

WISO DIREKT

19/2017

VERBRAUCHERDATENSCHUTZ IN DER DIGITALISIERUNG

Herausforderungen und Lösungsansätze

AUF EINEN BLICK

Der rasante technologische Wandel erfordert die Weiterentwicklung unseres Datenschutzverständnisses. Zeitgemäßer Datenschutz muss das informationelle Selbstbestimmungsrecht in der durch Digitaltechnik geprägten Welt gewährleisten. Er fördert einen fairen Umgang mit den Verbraucher_innen und sichert ihnen die Chance zur gesellschaftlichen Teilhabe. Moderner Verbraucherdatenschutz ermöglicht Verbraucher_innen, selbst darüber zu entscheiden, wem sie für welche Zwecke ihre persönlichen Daten zur Verfügung stellen.

Die von der Digitalisierung bewirkten Veränderungen sind global, sie umfassen alle Lebensbereiche und durchdringen sowohl die Arbeitswelt als auch den Alltag. Ausgehend von der klassischen Informationsverarbeitung (strukturierte Daten, Medien, Individualkommunikation) hat die Digitalisierung zum Sprung in die reale Welt angesetzt. Das Internet der Dinge, die Industrie 4.0 und die allgegenwärtige Datenverarbeitung bezeichnen Aspekte der umfassenden Verknüpfung der virtuellen mit der Kohlenstoff-Welt. Das Datenschutzrecht kann nur Antworten auf einen Teil der mit der Digitalisierung verbundenen Fragen geben. Nach klassischem Verständnis handelt es sich beim Datenschutz um ein „Abwehrrecht" der Bürger_innen gegen den Staat. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil von 1983 jedermann ein Recht zugesichert, selbst über die Verwendung der eigenen Daten zu entscheiden (Grundrecht auf informationelle Selbstbestimmung). Längst geht es aber nicht mehr allein um den Schutz gegen staatliche Machtansprüche. Es ist deshalb folgerichtig, dass die 2018 wirksam werdende Datenschutzgrundverordnung der Europäischen Union die Verarbeitung personenbezogener Daten durch staatliche und privatwirtschaftliche Stellen gleichermaßen reguliert.

HERAUSFORDERUNGEN

1. ÜBERWACHUNG

Den Menschen fällt es immer schwerer, nachzuvollziehen, wer was über sie erfährt und was mit den sie betreffenden Daten geschieht. Umfassende Überwachung gefährdet die Grundrechte auf Datenschutz und Privatsphäre. Analoge, in Büchern oder Akten abgelegte Informationen waren nur mit großem Aufwand auffindbar. Der Informationszugang setzte zudem den physischen Zutritt zu den Datenträgern voraus. In seinen Anfängen konzentrierte sich das Datenschutzrecht folgerichtig auf den Schutz vor unbefugtem Zugang zu Datenträgern und Datenverarbeitungseinrichtungen. Digitale Prozesse in vernetzten Infrastrukturen ermöglichen eine weitaus schnellere und effektivere Erschließung und Interpretation gespeicherter Daten, unabhängig von Zeit und Raum. Die Kehrseite der verbesserten Zugänglichkeit und leichten Erschließbarkeit ist der damit einhergehende Kontrollverlust. Auf digital gespeicherte Informationen kann jederzeit über Netze zugegriffen, Daten können unbemerkt kopiert und ohne größeren Aufwand reproduziert und verbreitet werden. Zudem bestehen umfassende Verknüpfungsmöglichkeiten. Biometrie (die Erkennung von Personen anhand bestimmter persönlicher Eigenschaften, etwa Gesichtsbild, Fingerabdruck, Iris) ermöglicht die vom Betroffenen unbemerkte Identifikation und Verknüpfung personenbezogener Daten. Überwachungsgefahren ergeben sich auch aus den in immer größerem Umfang entstehenden Metadaten. Jede digitale Transaktion hinterlässt Daten, die den Zeitpunkt, die Akteure, die Art und ggf. den Ort und weitere Umstände der Transaktion beschreiben. Durch die Digitalisierung unserer Alltagswelt, die Ausstattung von Fernsehern, Kühlschränken und Kraftfahrzeugen mit Prozessoren

>

FRIEDRICH EBERT STIFTUNG

und deren Vernetzung entstehen große Mengen derartiger Metadaten. Sie ermöglichen die Erschließung und Verknüpfung großer Informationsmengen und erleichtern deren automatisierte Auswertung einschließlich der Bildung von immer aussagekräftigeren Profilen. Diese wiederum sind Basis vieler erfolgreicher Geschäftsmodelle. Beunruhigend ist auch, dass das Interesse staatlicher Stellen an Daten zunimmt, die bei digitalen Dienstleistungen anfallen. Dies kommt etwa in der Forderung nach Aufschaltung der Polizei auf privat betriebene Videoüberwachungsanlagen und bei der bereits realisierten Vorratsdatenspeicherung von Telekommunikations- und Internetdaten zum Ausdruck.

2. BIG DATA - DIGITALE DISKRIMINIERUNG

Die Erzeugung, Zusammenführung und Analyse von immer mehr Daten aus den unterschiedlichsten Quellen (Big Data, Smart Data) soll das menschliche Verhalten transparent und vorhersagbar machen. Im Zentrum steht die Klassifizierung anhand von Scorewerten, wie sie schon seit längerer Zeit von Banken eingesetzt werden. Dabei wird eine Person zunächst elektronisch „vermessen", indem aus den über sie gesammelten Daten ein Profil erstellt wird. In dieses Profil gehen die unterschiedlichsten Parameter ein, etwa Angaben über das Alter, Geschlecht, Wohnlage, Wohnortwechsel, Anzahl der Mobilfunkverträge, Bankkonten, Kredite, Angaben aus Arbeits- und Mietverhältnissen, neuerdings auch Informationen aus sozialen Netzwerken. Das individuelle Profil wird mit statistischen Vergleichspersonen verglichen. Im Ergebnis wird den Betroffenen ein Scorewert zugewiesen, eine Art persönliche Kopfnote zur Bewertung der Kreditwürdigkeit. In Weiterentwicklung des Scoring geht es um das Erkennen komplexerer Korrelationsbeziehungen und deren Verwendung bei automatisierten Entscheidungen. Der Einsatzbereich derartiger Verfahren beschränkt sich nicht auf die Bewertung aller möglichen individuellen Risiken (etwa Zahlungsausfall, Krankheit, Tod). Ähnliche Methoden werden auch verwendet, um die Interessen und die Zahlungsfähigkeit und -bereitschaft potenzieller Kund_innen zu bewerten. Im Unterschied zu klassischen Risikobewertungen fließen in die Bewertung vielfach direkt oder indirekt auch Faktoren ein, die nach den Vorgaben des Gleichbehandlungsrechts nicht gegen die Betroffenen verwendet werden dürfen, etwa Geschlecht, ethnische Herkunft, Religion, Hautfarbe und sexuelle Orientierung. Die Folge sind erhebliche Diskriminierungsgefahren. Verbraucher_innen mit entsprechendem Profil können von Dienstleistungen und sonstigen Angeboten ausgeschlossen werden, etwa als Bewerber_in um eine Wohnung oder einen Arbeitsplatz.

3. PREISDIFFERENZIERUNG

Datenanalysen liefern auch die Grundlage für eine individualisierte Preisbildung. Dies ist heute schon bei Internetdiensten zu beobachten. In einer einfachen Version erfolgt die Preisdifferenzierung anhand der von den Nutzer_innen verwendeten Technik. Wer Apple nutzt, muss mehr zahlen als diejenigen, die den Online-Shop mit einem alten Windows-PC aufsuchen. Ausgefeilte Preisbildungsmechanismen funktionieren ähnlich wie das beschriebene Scoring. Dabei müssen etwa Verbraucher_innen mehr zahlen, aus deren Profil zu schließen ist, dass sie auf Grund einer Notsituation auf eine bestimmte Dienstleistung besonders angewiesen sind. Diese Methode ist umso wirksamer, desto mehr aktuelle Daten berücksichtigt werden. In die Datenanalyse können etwa Informationen aus E-Mails, aufgerufene Webseiten, genutzte Apps, in der Cloud gespeicherte Dokumente, Suchanfragen und Einträge in elektronischen Terminkalendern einfließen. Hier sind Plattformen wie Google im Vorteil, die sich den übergreifenden Zugriff auf die von ihren Kund_innen gespeicherten Daten einräumen lassen. Systeme mit nach Interessenlage und Zahlungsbereitschaft differenzierten Preisen könnten demnächst auch im Supermarkt Einzug halten. Schon haben Supermarktketten damit begonnen, ihre Waren mit elektronischen Preisschildern auszustatten. Damit werden zunächst sogenannte „Flatterpreise" möglich, die – ähnlich wie die Benzinpreise an den Tankstellen – nach Tageszeit fluktuieren. Wenn die Warenwirtschaftssysteme des Einzelhandels mit den Profiling-Systemen verbunden werden, sind auch im Supermarkt individualisierte Preisangaben möglich. Statt eines Einheitspreises wird ein individueller Preis eingeblendet, wenn sich ein/e bestimmte/r Verbraucher_in nähert. Es ist zu befürchten, dass für viele Verbraucher_innen negative Verteilungseffekte auftreten und die Preistransparenz dabei verloren geht.

4. LOCK-IN-EFFEKTE

Der Geschäftserfolg digitaler Plattformen wird nicht allein durch die Qualität der einzelnen Dienstleistung bestimmt. Gerade bei kommunikativen Diensten steigt der individuelle Nutzen mit der Zahl der Personen, die einen Dienst in Anspruch nehmen. Dieser Netzwerkeffekt ist seit der Erfindung des Telefons bekannt. Sein weltweiter Erfolg wurde nur deshalb möglich, weil sich frühzeitig gemeinsame Standards durchsetzten, die gewährleisten, dass die Kommunikation unabhängig vom Anbieter und vom Standort der Nutzer_innen funktioniert. Im Internet folgten die E-Mail-Kommunikation und das World Wide Web diesem Modell. In der letzten Dekade waren allerdings solche digitalen Geschäftsmodelle besonders erfolgreich, die nach dem Prinzip der geschlossenen Benutzergruppe funktionieren. Paradebeispiele für solche geschlossenen Systeme sind Soziale Netzwerke und Messengerdienste. Sie gestatten die Kommunikation nur zwischen den eigenen Mitgliedern. Während wir vom Telekom-Handy ein im Vodafone-Netz eingebuchtes Smartphone anrufen können, können ein WhatsApp-Nutzer_innen nur mit anderen WhatsApp-Nutzer_innen Nachrichten austauschen. Digitale „Freundschafts"-Beziehungen sind nur innerhalb des jeweiligen digitalen Biotops möglich. Wer zu einem anderen Anbieter wechselt, muss auf seine Freunde bzw. Follower verzichten. Für die Nutzer_innen ist es deshalb sehr unattraktiv, von einer Plattform auf eine andere zu wechseln. Die durch derartige Einschließungs- bzw. Lock-in-Effekte erreichte stärkere Kundenbindung ermöglicht es den Unternehmen, den Mitgliedern einseitig die Bedingungen zu diktieren, unter denen ihre Daten verarbeitet und ausgewertet werden. Der Geschäftserfolg der Dienste bzw. Plattformen basiert ganz wesentlich darauf, dass sie die Daten und die Auswertungsalgorithmen exklusiv nutzen, vielfach ohne die eigentlichen Datenproduzenten – neben den Nutzer_innen auch die Urheber_innen von Inhalten – daran zu beteiligen. Besonders kritisch ist es, dass systematisch und sehr erfolgreich versucht wird, die Nutzer möglichst zu

kontrollieren, ihr Verhalten und ihre Vorlieben zu erfassen. Es ist deshalb von zentraler Bedeutung für den Verbraucherdatenschutz, Lock-in-Effekte zu durchbrechen und eine ungehinderte Kommunikation über Plattformgrenzen hinweg zu gewährleisten.

5. DIGITALES GESUNDHEITSWESEN

Die Digitalisierung macht um die Arztpraxis und das Krankenhaus keinen Bogen. Dies ist datenschutzrechtlich deshalb bedeutsam, weil dort die sensibelsten personenbezogenen Daten verarbeitet werden. Aus gutem Grund gelten die Informationen, die die Ärzt_innen bei der Krankenbehandlung erfahren, seit Menschengedenken als äußerst schutzwürdig. Schließlich sind die medizinischen Risiken, die mit dem Betrieb digitaler medizinischer Geräte einhergehen, für die Betroffenen vielfach existenziell. So können fehlerhafte Messwerte schwer wiegende Therapiefehler zur Folge haben. Angesichts des hohen Schutzbedarfs von Gesundheitsdaten und der ernsten Konsequenzen von Datenschutzverletzungen müssen im Gesundheitswesen besonders hohe Schutzstandards gewährleistet werden. Die bei digitalen medizinischen Geräten anfallenden Daten müssen in besonderem Maße gegen unberechtigten Zugang, Veränderung und Löschung geschützt werden. Die jüngsten Fortschritte in der Genomanalyse und in der medizinischen Analytik sind zum Teil nur deshalb möglich geworden, weil medizinische und genetische Massendaten automatisiert ausgewertet wurden. Im Grunde bedienen sich derartige Analyseverfahren ähnlicher (Big Data-) Algorithmen, wie sie beim Marketing zum Einsatz kommen. Bei derartigen Verfahren besteht eine erhebliche Gefahr von Nachteilen für die Betroffenen, etwa wenn Personen wegen ihrer genetischen Disposition von Versicherungsleistungen ausgeschlossen werden. Eine weitere Herausforderung sind „Fitness Tracker" und vergleichbare freiverkäufliche Geräte. Abgesehen von dem bisweilen fragwürdigen medizinischen Nutzen muss auch hier gewährleistet werden, dass die erzeugten Gesundheitsdaten nicht in die falschen Hände geraten. Besonders problematisch ist es, dass bei vielen Produkten sämtliche Daten in Cloud-Services ohne angemessenes Datenschutzniveau gespeichert werden. Zudem lassen sich manche Anbieter durch allgemeine Nutzungsbestimmungen das Recht zur umfassenden, für die Betroffenen intransparenten Datenverwendung einräumen.

6. DIGITALE MOBILITÄT

Den wenigsten Autofahrer_innen ist bewusst, in welchem Umfang moderne Fahrzeuge schon heute Daten sammeln. Unter anderem werden Abstellpositionen der Fahrzeuge chronologisch gespeichert, so dass sich die zurückgelegten Strecken rekonstruieren lassen. Ebenso gespeichert werden eine Vielzahl von Fahrparametern, etwa die Drehzahl, die Beschleunigung und Angaben zu Bremsaktivitäten und Daten aus diversen Fahrassistenzsystemen. Hinzu kommen immer mehr Daten aus Navigations- und Entertainmentsystemen. Schließlich müssen nach EU-Vorgaben in Neuwagen Notfallsysteme eingebaut werden, die bei Unfällen automatisiert Rettungsstellen und Polizei kontaktieren (eCall). Noch weitaus umfangreicher werden die Daten sein, die beim autonomen Fahren anfallen. Umstritten ist, wo die Grenzen zwischen personenbezogenen und nicht personenbezogenen Daten exakt verlaufen und wer die Verfügungsmacht über die Daten hat. Auch vordergründig technische Daten weisen häufig Personenbezug auf. Technische Daten, die dem Halter oder Fahrer zugeordnet werden können und Aussagen über sein Verhalten oder seine Präferenzen ermöglichen, sind personenbezogen. Dem Hersteller und der Werkstatt ist es grundsätzlich möglich, die in immer größerem Umfang anfallenden technischen Angaben mittels der Fahrzeugidentifikationsnummer den Halter_innen zuzuordnen. Daneben gibt es allerdings auch technische Angaben, die keinen Bezug zum individuellen Verhalten aufweisen und die ausschließlich für datenschutzrechtlich unproblematische Zwecke gesammelt werden, etwa zur Qualitätskontrolle und zum Signalisieren von Fehlfunktionen. Auch Daten, die vom Hersteller oder der Werkstatt nicht ausgelesen werden können, sind weniger sensibel. Aber angesichts der zunehmenden Vernetzung ist dies immer mehr die Ausnahme. Immer mehr Unternehmen haben ein wirtschaftliches Interesse an den Daten. Auch Dritte setzen zunehmend auf Anwendungen, die auf der Auswertung von Daten über das Fahr- und Nutzungsverhalten basieren. So bieten einige Versicherungen inzwischen Telematiktarife an, bei denen Halter_innen mit „vorsichtigem" Fahrverhalten Rabatte eingeräumt werden. Schließlich sind weltweit tätige Unternehmen wie Google mit datenorientierten Geschäftsmodellen daran interessiert, die Mobilitätsdaten als zusätzliche Quelle zu nutzen. Vor diesem Hintergrund sind technische und rechtliche Schutzvorkehrungen erforderlich, um die Nutzer_innen und Halter_innen vor umfassender Ausforschung zu schützen.

ZEITGEMÄSSER DATENSCHUTZ

1. DATENSCHUTZ ALS VERTRAUENSANKER

Datenschutz ist mehr als ein notwendiges Übel. Die sich häufenden Berichte über Datendiebstähle, Hacking-Vorfälle und Virenattacken belegen die Verletzlichkeit vernetzter digitaler Systeme. Umfragen belegen die negativen Auswirkungen des gestörten Vertrauens in elektronische Dienstleistungen. So ist die Nutzung des Online-Banking in mittelständischen Unternehmen trotz fortgesetzter Digitalisierung rückläufig. Nachgewiesener Datenschutz kann dieser Negativtendenz entgegenwirken. Technische Produkte mit effektivem Schutz gegen Manipulation und Überwachung haben gegenüber schwächeren Konkurrenzprodukten einen Wettbewerbsvorteil. Datenschutzgütesiegel und die Zertifizierung von Diensten und Produkten entsprechend der Europäischen Datenschutzgrundverordnung dokumentieren die Datenschutzkonformität und eröffnen neue Möglichkeiten für das Marketing.

2. TECHNOLOGISCHER DATENSCHUTZ

Grundlegende rechtliche und ethische Anforderungen müssen in der Technik verankert werden. Es reicht nicht aus, die Schutzvorkehrungen nachträglich auf fertige Systeme und Infrastrukturen aufzupfropfen. Sofern dies überhaupt gelingt, sind nachträgliche Änderungen meist sehr schwierig, fehleranfällig und kostspielig. Viel sinnvoller ist es, die entsprechenden Anforderungen bereits in einer sehr frühen Phase der Systementwicklung zu berücksichtigen (Privacy by Design). Zu den wichtigsten Instrumenten des

technologischen Datenschutzes gehört die Anonymisierung personenbezogener Daten. Insbesondere bei Big-Data-Analysen lassen sich mit anonymisierten oder unter Pseudonym verarbeiteten Daten vergleichbare Ergebnisse erzielen wie bei der Verwendung von Daten, die direkt mit einer Person verknüpft sind. Angesichts zunehmender Risiken sollten digitale Systeme grundsätzlich schon im Auslieferungszustand Datenschutz und Datensicherheit gewährleisten (Privacy by Default, Security by Default). So sollten bei Smartphones die Ortungsfunktionen standardmäßig deaktiviert sein. Die Besitzer_innen sollten die Möglichkeit haben, diese und andere Funktionen gezielt zu aktivieren, soweit sie entsprechende Dienste nutzen wollen (z. B. Navigation). Angesichts zunehmender Vernetzung und steigender Abhängigkeit unserer Gesellschaft von digitalen Techniken gewinnen auch Schutz vor unberechtigter Kenntnisnahme, vor Manipulation und unbefugter Löschung bzw. Blockierung von Daten an Bedeutung. Schließlich sollten Datenschutztools die Nutzer_innen dabei unterstützen, ihre Daten effektiv zu sichern: Beispiele hierfür sind Apps zum Selbstschutz gespeicherter oder übertragener Daten (insb. Datenverschlüsselung) und zur Prüfung und Bewertung elektronischer Angebote (Tools zur Prüfung der Datenschutzeigenschaften und der IT-Sicherheit eines Dienstes). Die Entwicklung von Datenschutztools sollte auf europäischer und deutscher Ebene gefördert werden.

3. ZEITGEMÄSSES DATENSCHUTZRECHT

Mit der Datenschutzgrundverordnung, die am 25. Mai 2018 wirksam wird, wurde auf europäischer Ebene eine gute Basis für ein zeitgemäßes Datenschutzrecht gelegt. Das „Marktortprinzip" soll gewährleisten, dass die Datenschutzvorgaben auch für die Anbieter gelten, die außerhalb der Europäischen Union ihren Sitz haben. Die Grundverordnung enthält neben den klassischen Grundsätzen der Erforderlichkeit und Zweckbindung auch Vorgaben zum technologischen Datenschutz (Data Protection by Design, Datenschutz-Folgenabschätzung) und neue Instrumente zum Nachweis der Datenschutzkonformität von Produkten und Diensten (Zertifizierung, Datenschutz-Gütesiegel). Die Datenschutzrechte der Betroffenen auf Auskunft, Sperrung und Löschung wurden ergänzt um ein „Recht auf Vergessenwerden", das – der Rechtsprechung des Bundesverfassungsgerichtes und des europäischen Gerichtshofs folgend – eine unbeschränkte Weiterverbreitung falscher oder inaktueller persönlicher Informationen über das Internet untersagt. Neu ist auch das Recht auf Datenportabilität. Die Nutzer_innen bekommen dadurch einen Anspruch auf Herausgabe ihrer Daten in maschinenlesbarer und wiederverwendbarer Form. Dies reicht jedoch nicht aus, um Lock-in-Effekte zu verhindern, die dem Datenschutz schaden und den Wettbewerb behindern. Erforderlich ist eine ergänzende Verpflichtung zur Interoperabilität von Kommunikationsdiensten, etwa im Telekommunikationsrecht. Das Datenschutzrecht muss auf Basis der Datenschutzgrundverordnung weiterentwickelt werden. Aktuell wird über eine neue EU-Datenschutzverordnung für elektronische Kommunikationsdienste diskutiert. Sie soll wirksame Vorgaben gegen die umfassende Registrierung des Nutzungsverhaltens im Internet enthalten. So ist etwa zu gewährleisten, dass sich die Internetanbieter an die Do-Not-Track-Vorgaben der Nutzer_innen in den Browsereinstellungen halten. Das Recht, verschlüsselt zu kommunizieren, darf nicht eingeschränkt werden. In Deutschland besteht Handlungsbedarf bei den bereichsspezifischen Datenschutzbestimmungen, etwa beim Schutz der Sozial- und Gesundheitsdaten und beim Beschäftigtendatenschutz. Die Regelungen zum Einsatz von Scoringverfahren sollten weiterentwickelt und in das deutsche und europäische Verbraucherrecht übernommen werden. Notwendig sind deshalb Vorgaben im Verbraucherschutzrecht, um die Markttransparenz zu gewährleisten.

FAZIT

Die Digitalisierung hat erhebliche Auswirkungen auf die Gesellschaft: Neben zahlreichen positiven Effekten drohen der Verlust der Privatsphäre und der informationellen Selbstbestimmung. Die digitale Daten- und Machtkonzentration ist mit Manipulationsgefahren verbunden. Zudem ergeben sich Diskriminierungseffekte, wenn auf großen Datenmengen basierende Entscheidungen getroffen werden. Datenschutz ist daher auch eine Gerechtigkeitsfrage. Es wäre fatal, wenn das Einkommen darüber entscheidet, wer sich Privatsphäre noch leisten kann. Es besteht erheblicher gesellschaftlicher Gestaltungsbedarf auf rechtlicher, wirtschaftlicher und politischer Ebene. Die Verzahnung des Datenschutz-, Verbraucher- und Wettbewerbsrechts ermöglicht Synergien, die erschlossen werden müssen. Die mündigen Verbraucher_innen können ihre Entscheidungen nur dann souverän treffen, wenn sie sich in der digitalen Gesellschaft zurechtfinden. Deshalb ist zeitgemäßer Verbraucherdatenschutz auch eine Herausforderung für unser Bildungswesen.

Autor

Peter Schaar ist Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz, Berlin.

Impressum

© 2017
Friedrich-Ebert-Stiftung
Herausgeberin: Abteilung Wirtschafts- und Sozialpolitik
Godesberger Allee 149, 53175 Bonn
Fax 0228 883 9202, 030 26935 9229, 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

ISBN: 978-3-95861-849-7