AK POLICY PAPER

BIG DATA UND VERBRAUCHERSCHUTZ

Daniela Zimmer

April 2017

Das wichtigste auf einen Blick:

- Im Trend: Autos, Heizungen, Laufschuhe, Puppen, Uhren, Zahnbürsten u.v.m., sammeln permanent Betriebsinformationen und damit Verhaltensdaten über Nutzer. Auch Daten, die anonymisiert Scheinen lassen sich mit passenden Analysewerkzeugen fast immer einer Person eindeutig zuordnen.

- Der zeitgeistige Begriff „Datenkapitalismus“ beschreibt, wie über unser Alltagsverhalten des „Always on“ („rund um die Uhr online“) bis dato noch nicht mess- und verwertbarer Teile des Lebens monetarisiert werden. Die Analyse der von Alltagsgeräten erzeugten gigantischen Datenmengen gilt als Wachstumshoffnung. Kommerzialisierung durchdringt so letzte, geschützte Bereiche der Privatsphäre.

- Mit „Datamining“ wird nach unentdeckten Zusammenhängen und Verhaltensmustern in großen Datenbeständen gesucht. „Big Data“-Analysen können die Selbstbestimmung der Betroffenen in Bezug auf ihre Daten immens gefährden. Die Klassifizierung von Personen (-gruppen) anhand statistisch berechneter Merkmale führt zu ethischen und rechtlichen Problemen: die vielen Facetten sozialer Wirklichkeit lassen sich nicht allein in algorithmisch berechneten Werten ausdrücken. Es besteht die Gefahr stereotyper Diskriminierung.

- Nicht zuletzt in den Händen großer Internetkonzerne werden Big Data-Anwendungen als Herrschaftsinstrument und als Anlass betrachtet, die Frage nach den gesellschaftlichen Machtverhältnissen neu zu stellen: Wer garantiert in der Datenökonomie den Betroffenen den freien Willen? Und wer kontrolliert die Datenbarone?

Worum es geht

Big Data als Wachstumshoffnung: Digitalisierung ermöglicht globalen Datentransfer nahezu in Echtzeit. Konsum- und Finanzmärkte agieren software- und datenbasiert, womit es unternehmensseitig naheliegt, die ohnehin anfallende Daten - Verbindungsdaten im Mobilfunk, Überweisungsdaten im Bankgeschäft, Pulsfrequenz-Messdaten aus dem Fitnessarmband, Fahrverhaltensdaten aus der Telematik-Box im Auto oder Twitter-Meldungen - interessensgeleitet auswerten zu wollen. „Schon vor unserer Geburt sind wir mit Ultraschallfotos online“, beschreibt die FAZ den digitalen Konsumentenalltag: „Wir kaufen nicht nur ein Produkt, wir werden selbst zum Produkt.“ Das Wissen um unser Verhalten – was wir kaufen, lesen, denken, wo wir uns bewegen – hat Warencharakter angenommen. Datenschutzrecht und Aufsichtsbehörden sind immer seltener in der Lage, die gegenläufigen Interessen an einer Datennutzung und Geheimhaltung wirksam und fair auszubalancieren.

Immer mehr Alltagsgeräteerzeugen Daten. Billige Speichertechnologie trägt dazu bei, dass Daten unbegrenzt gespeichert, analysiert, kombiniert und ökonomisch verwertet werden können. Das „Internet der Dinge“ gilt als Wachstumstreiber in Zeiten stagnierender Wirtschaft. Big Data Analysen sollen bis 2020 das europäische Wachstum um 1,9% ankurbeln. Im selben Jahr sollen 32 Milliarden Gegenstände weltweit mit dem Internet verbunden sein. „Nur“ fünf Prozent aller digitalen Daten werden aber (laut EMC-Digital-Universe-Studie) derzeit ausgewertet. Wirtschaft, Wissenschaft und nicht zuletzt den Staat interessiert deshalb: Wie können wir die Datenberge besser nutzen? Die EU-Kommission forciert einen europäischen Binnenmarkt für Datenflüsse. Dieser sei Voraussetzung einer „pulsierenden wissensbasierten Gesellschaft“.

Beispiele: Anschaulich illustriert das aktuelle Schutzbedürfnis privater Haushalte das Beispiel von Cayla, der „Spionin im Kinderzimmer". Sie sei „fast wie eine richtige Freundin", steht auf der Produktwebsite jener Puppe, die via Bluetooth-Verbindung und Spracherkennung auf Fragen antwortet und Unterhaltungen zwischen Kind und Puppe an den US-Hersteller weiterleitet. Sie zeigt beispielshaft jene Probleme, die mit dem schnell wachsenden Markt vernetzter Haushaltsgeräte verbunden sein werden: versteckte Abhöreigenschaft und Intransparenz der Datenempfänger. Ein leichtes Hacking-Opfer ist die Puppe angesichts ungesicherter Verbindungen obendrein. Es finden sich aber auch Innovationsbeispiele von unbestreitbarem gesellschaftlichen Nutzen: Die Vereinten Nationen erkennen drohende Infektionen, Hungersnöte oder Unruhen über ganze Länder hinweg dadurch viel früher, dass Millionen öffentlicher Kurznachrichten mit Fotos und Videos auf Knopfdruck ausgewertet werden.

Die Anwendungen reichen letztlich von A wie Autos, deren elektronische Assistenzsysteme permanent Daten liefern, bis Z wie intelligente Zahnbürsten, deren Hersteller mit Nutzungsdaten handeln können. Smarte Armbänder überwachen Aktivitäten und Fitness des Trägers und übertragen die Resultate der Körpervermessung an Gesundheitsdienstleister. Haushalte sind fernbedienbar, denn auch Heizung, Kühlschränke, Backöfen, Kaffeemaschinen, Badewannen, Rohrbruch- oder Feuermelder werden mit vernetzten Sensoren ausgestattet. Auf Straßen und in Gebäuden sind Sensoren allgegenwärtig, um Verkehrsströme zu erfassen und Personen bzw. Fahrzeuge zu leiten. In öffentlichen Verkehrsmitteln wird die Auslastung über deren Handy-ID festgestellt und Festivalveranstalter überwachen auf dieselbe Weise den Besucherandrang.

Das Fraunhofer Institut sieht praktisch alle Wirtschaftszweige, Institutionen und jeden digitalen Nutzer durch das kommerzielle Innovationspotenzial von Big Data berührt. Myriaden an Objektdaten werden über Zeit fürs Marketing, den wissenschaftlichen Erkenntnisgewinn aber auch die staatliche Planung und Kontrolle u.v.m. zur Verfügung stehen und müssen nicht mehr mühsam erhoben werden. Über die Auswertung des Nutzerverhaltens lassen sich standardisierte Produkte, Services aber auch die Verkaufspreise erstmals individualisieren. Konsumenten mit Verhaltensweisen, die mit Blick auf Kosteneffizienz und Risikovorbeugung unerwünscht sind, werden „aussortiert."

Wesentliche Erkenntnisse

Soziale Folgen: Die Perfektionierung der Suche nach unentdeckten Mustern und Zusammenhängen in großen Datenbeständen höhlt Datenschutz und Privatsphäre aus. Denn Grundrechtsprinzipien wie Datensparsamkeit, strikte Bindung an vorab festgelegte Erhebungszwecke, Weiterverarbeitungsverbote und das Verbot der Vorratsdatenspeicherung lassen sich mit Big Data-Analytik nur selten in Einklang bringen. Betroffene können die kommerziellen Verwertung ihrer Daten kaum durchschauen. Im Gegensatz zu den NutzerInnen sind die Unternehmen selbst alles andere als transparent. Welche Daten zur Analyse herangezogen werden und welche Algorithmen dabei eine Rolle spielen, wird ungern preisgegeben. Problematisch werden solche statistischen Analysen vor allem dann, wenn sie im Einzelfall zu konkreten Konsequenzen führen, etwa, wenn durch Profiling die persönliche Kreditwürdigkeit beurteilt wird. Dann kann es schon vorkommen, dass ein Kreditantrag automatisiert abgelehnt wird, weil zufällig die Wohngegend ein höheres Risiko vermuten lässt, auch wenn die tatsächliche Lebenssituation der Betroffenen ganz anders ist. Bislang rein finanzielle Bonitätsbewertungen von Konsumenten könnten zu einem „Social Scoring" und „Predictive Policing" (Vorhersage von Verhaltensabweichungen) ausgeweitet werden.

Big Data oft mit Personenbezug: Beim Internetsurfen fallen permanent sogenannte „Metadaten" (Verbindungs- und Standortdaten, IP-Adresse usw.) an. Sie wirken nicht wie persönliche Informationen. Der Eindruck täuscht aber. Mit wenig Aufwand konnten Forscher (des MIT) aus einer Million Angaben über bloß den Tag, Ort und die Höhe von Kreditkartenzahlungen Zuordnungen zu einzelnen Personen treffen. Auf EU-Ebene wird die Frage, wem gehören die vorgeblich nicht personenbezogenen Betriebsdaten von smarten Fahrzeugen und Konsumartikeln diskutiert. In diesem Eigentumskonflikt zwischen Geräteherstellern und Softwarelieferanten wird der Konsument bewusst übersehen. Ein vernetztes Auto erzeugt aber nicht nur technische Daten, an denen Rechteinhaber geistiges Eigentum begründen. Soweit Gerätedaten einen Personenbezug aufweisen, darf aus Sicht von Verbraucher- und Datenschützern nur ein Stakeholder - nämlich der Konsument – selbstbestimmt über ihre Verwendung entscheiden.

Forderungen

Datenschutzgrundverordnung verbessern: Die EU hat sich auf ein Datenschutzkonzept geeinigt, das ab 2018 das bisherige Schutzniveau in Österreich absenken dürfte. So soll Datenverarbeitung, an der ein berechtigtes Interesse besteht, auch ohne Zustimmung der Betroffenen erlaubt sein. An Stelle des Vorrangs für den Datenschutztritt die allgemeine Anerkennung eines Verwertungsinteresses an persönlichen Daten. Vor allem aber wurde das Prinzip der Zweckbindung zum Auslaufmodell erklärt. Dieses hält den Datennutzer, die Datennutzerin dazu an, sich auf jene Daten zu beschränken, die für die Erfüllung des konkret benannten Zwecks erforderlich sind. Enge Zweckbindung steht freilich dem Wesen von Big-Data-Anwendungen diametral entgegen, die auf möglichst großen Datenmengen basieren und nach unbekannten Zusammenhängen und zufälligen Verwertungsmöglichkeiten suchen. Daten dürfen also künftig für andere als den ursprünglichen Zweck weiterverarbeitet werden.

Schlagkräftige Datenschutzkontrolle: Derzeit leidet der Datenschutz an Vollzugsdefiziten. Ressourcenschwache Datenschutzbehörden können keinen Marktüberblick über millionenfache und zum Teil höchst komplexe Verarbeitungsvorgänge behalten. Um den Vollzug zu verbessern, braucht es unabhängige Datenschutzbeauftragte (unabhängig von der Unternehmensgröße) und wirksamere Kontrollbehörden. Eine Pflicht zur Risikofolgenabschätzung durch den Datenverwender selbst und datenschutzfreundliche Voreinstellungen bei Geräten, Diensten und Software sind zukunftsweisende Ansätze – allerdings nur, wenn die Kontrolle dem Kontrollierten nicht alleine überlassen bleibt. Die Datenschutzgrundverordnung sieht die Option einer Verbandsklagsbefugnis für die Mitgliedstaaten vor. Der österreichische Gesetzgeber soll von dieser Möglichkeit Gebrauch machen und für Organisationen wie die AK und die Gewerkschaften entsprechende kollektive Klagsbefugnisse gegenüber Unternehmen vorsehen, die Datenschutzverstöße begehen.

e-Privacy-Verordnung: e-Privacy bedeutet vor allem „Do not track“ (Datenspuren im Internet zu vermeiden). Der gleichnamige Entwurf einer EU-Verordnung schützt Konsumenten zu wenig und muss nachgebessert werden. Browserhersteller sollten ihre Produkte standardmäßig datensparsam voreinstellen müssen. Nicht nur der Zugriff auf Endgeräte durch „Spionage“-Software ist regelungsbedürftig. Internetnutzer sind auch in Bezug auf die damit verbundene Erstellung von Nutzungsprofilen schutzbedürftig. Die Nutzbarkeit von Verkehrs- und Standortdaten durch Internetprovider darf über das bisherige Maß (Netzsicherheit, Gebührenabrechnung, Vermarktung von eigenen Kommunikationsdiensten jeweils mit vorheriger Zustimmung des Nutzers) nicht hinausgehen. Handynutzer, die sich in Geschäften aufhalten, dürfen nicht ohne ihre Zustimmung durch Minifunkchips ausgespäht werden.

Transparenz für Algorithmen: Algorithmen treffen immer öfter Vorhersagen über das künftige Verhalten von Personen. Die hinter Algorithmen stehenden Regeln, Gewichtungen und einfließenden Datenarten müssen verständlich erklärt weden, wenn sich aus einer Bewertung oder Prognose nachteilige Folgen für Betroffene ergeben können (Vertragsverweigerung, schlechtere Konditionen, Benachteiligung am Arbeitsmarkt u.v.m.) Die Methoden sollten durch unabhängige Aufsichtsstellen in Form eines „Algorithmen-TÜVs“ auf ihre wissenschaftliche Haltbarkeit geprüft und zertifiziert werden. Daten, die zweckfremd erhoben wurden (zB Facebookeinträge) dürfen nicht für Personenbewertungen verarbeitet werden. Dienste, die zur grundlegenden Daseinsvorsorge gehören, sind von Profilings jedenfalls auszunehmen.

Daten und Verbrauchervertragsrecht: Auch verbrauchervertrags- und wettbewerbsrechtliche Probleme rund um das Eigentum an Daten des „Internets der Dinge“ sind zu klären. Der Zugriff auf die Daten darf nicht nur dem Hersteller vorbehalten sein. Konsumenten dürfen nicht gezwungen werden, Services nur von diesem zu beziehen. Es darf nicht untersagt sein, smarte Geräte selbst zu reparieren oder einer unabhängigen Werkstatt zur Reparatur zu überlassen. Bei vernetzten Produkten müssen Konsumenten deshalb

- in jeder Hinsicht autonom über das gekaufte Produkte verfügen können
- Eigentum haben an allen eingebauten Softwarekomponenten
- ein uneingeschränktes Selbstbestimmungsrecht haben über alle Daten, die das gekaufte Produkt erzeugt

- ohne jeden Zwang darüber entscheiden können, ob und wem sie diese Daten zugänglich machen ihre Werkstätten in jeder Hinsicht frei wählen dürfen
- nicht gezwungen sein, Koppelungsverträge zu akzeptieren (Warenkauf plus Wartungs- und Serviceverträge, Drittanbieterdienste oder Versicherungsangebote, die ein Tracking der Produktbenutzung beinhalten) und
- darauf vertrauen dürfen, dass der Hersteller oder Verkäufer sich nicht auf Haftungs- und Gewährleistungsausschlüsse berufen kann, wenn der Verbraucher sich seine Werkstätte frei aussucht oder nicht alle anfallenden Daten zugänglich macht.

Wichtige Quellen und Verweise auf weiterführende Literatur/Unterlagen und Links zum Thema

Cracked Labs, Wolfie Christl, Studie im Auftrag der AK (2014): Kommerzielle digitale Überwachung im Alltag - Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data; https://media.arbeiterkammer.at/PDF/Digitale_Ueberwachung_im_Alltag.pdf

Institut für Technikfolgenabschätzung der Akademie der Wissenschaften, Robert Rothmann, Jaro Sterbik-Lamina, Walter Peissl; Studie in Kooperation mit der AK (2014): Credit-Scoring in Österreich. https://media.arbeiterkammer.at/wien/PDF/studien/Credit_Scoring_2014.pdf

Institut für Technikfolgenabschätzung der Akademie der Wissenschaften, Jaro Sterbik-Lamina, Walter Peissl; Studie in Kooperation mit der AK (2012): Geodatenutzung auf mobilen Endgeräten. https://media.arbeiterkammer.at/PDF/Studie_Geodaten.pdf

Schlussfolgerungen des Norwegian Consumer Council (NCC) zu internetbasiertem Spielzeug wie der “Puppe Cayla” (2016): https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

EMC Deutschland GmbH, EMC Digital Universe Studie (2014):„Digitales Universum explodiert durch Sensordaten“: http://www.presseportal.de/pm/8234/2709706

Bayrische Landeszentrale für neue Medien (BLM): Infobroschüre (2017) „Dein Algorithmus-meine Meinung!“ Algorithmen und ihre Bedeutung für Meinungsbildung und Demokratie https://www.blm.de/aktivitaeten/medienkompetenz/materialien/algorithmenbroschuere.cfm

Massachusetts Institute of Technology (MIT), Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, Alex Pentland: Studie (2015) “Unique in the shopping mall: On the reidentifiability of credit card metadata”;
http://www.datenschutzticker.de/2015/02/einkaufen-mit-der-kreditkarte-verraet-identitaet-des-nutzers/
bzw.
http://science.sciencemag.org/content/347/6221/536.full

Institute of Information Systems Humboldt University Berlin, Sarah Spiekermann: Fachartikel (2013) „Individual Price Discriminaton – An impossibility?“; http://ec-wu.at/spiekermann/publications/individual%20price%20discrimination.pdf