Machtkämpfe um Big Data Bürger und Verbraucher müssen geschützt werden

Lena Ulbricht

Summary: Big Data makes us reconsider the power relations in modern societies. It is a form of regulation that generates individualized rules, conflates rule setting and rule implementation and is opaque. Big Data can therefore improve the effectiveness and efficiency of regulation, but poses risks for the autonomy of rule takers and rule executers. In order to act as opponents of the big data based corporations, regulators from data protection, consumer protection and anti-trust regulation need to join forces.

Kurz gefasst: Big Data stellt die Frage nach gesellschaftlichen Machtverhältnissen neu. Es ist eine Form der Regulierung, die stark nach Subgruppen differenziert, Regelsetzung und -implementierung zusammenfasst und wenig transparent ist. Es kann also Effektivität und Effizienz verbessern, schränkt aber zugleich Selbstbestimmung ein, nicht nur bei Regeladressaten, sondern auch bei Regelanwendern. Für eine effektive Regulierung von Big Data müssen sich Datenschützer, Marktwächter und Verbraucherschützer zusammenschließen, wenn sie als Gegengewicht zu den großen Konzernen der Datenökonomie auftreten wollen.

Mit dem Schlagwort „Big Data" vermarkten Unternehmen datenbasierte Produkte, Politiker versprechen eine rationalere Politik, und Wissenschaftlerinnen wollen damit Forschungsmittel einwerben. Was spricht dafür, sich Big Data, der automatisierten Auswertung von Daten, die massenhaft im Zuge der Digitalisierung anfallen, in einem sozialwissenschaftlichen Forschungsprojekt zu widmen?

Big Data ist ein Ausdruck gesellschaftlicher Auseinandersetzungen über die Gestaltung der Digitalisierung und somit über Machtverhältnisse. Wenn man Regulierung als die absichtsvolle Setzung und Implementierung von Regeln versteht, ist Big Data eine Form der Regulierung, gleichzeitig aber auch Gegenstand der Regulierung. Was lehrt uns Big Data über Regulierung und gegenwärtige Auseinandersetzungen um Macht?

Big Data wird dafür genutzt, Regeln zu setzen und deren Umsetzung zu gewährleisten. Befürworter erwarten, dass Big Data Regulierung effektiver, effizienter und auch gerechter macht. Kritiker sehen in Big Data stattdessen ein Vehikel, mit dem eine zunehmende Überwachung und Kontrolle von Bürgern und Verbraucherinnen vorangetrieben wird.

Diese Kontroverse lässt sich anhand der „Passenger Name Records" (PNR) verdeutlichen. Hierbei handelt es sich um Daten über Reisende, die in vier global betriebenen kommerziellen Datenbanken gesammelt werden. Reiseveranstalter, Fluggesellschaften und weitere Partner pflegen Daten ein, über Reisende, deren Routen, Mitreisende, Kontaktdaten, Buchungs- und Zahlungsdaten. Reiseveranstalter benötigen die PNR, um die verschiedenen Elemente einer Reise integriert zu organisieren, etwa verschiedene Verkehrsmittel, Hotels, Mietwagen etc. Aber auch Regierungen werten die Daten für sicherheitspolitische Entscheidungen aus, wie etwa in den USA, Kanada und Australien. Seit 2017 können auch alle EU-Staaten die PNR für Flüge zwischen der EU und dem EU-Ausland sowie für ausgewählte innereuropäische Flüge analysieren.

Die staatlichen Sicherheitsbehörden durchsuchen die Daten nach Faktoren, mit denen sie Personen klassifizieren, um so mutmaßlich unerwünschten Reisenden die Einreise verweigern zu können: Drogenkurieren, Terroristen, illegalen Einwanderern oder Personen, die zu solchen werden könnten. Der Clou an dieser Auswertung liegt den Sicherheitsbehörden zufolge darin, dass sie nicht mehr darauf angewiesen sind, die Identität eines Terroristen zu kennen, um diesen am Flughafen zu verhaften. Vielmehr erlaubt es das *data mining*, die Suche nach neuen Mustern in großen Datensätzen, Menschen anhand ihres Reiseverhaltens als potenzielle Terroristen oder Kriminelle zu identifizieren. Big Data setzt hier Regeln, indem es Reisende in Risikogruppen teilt und ihre Reisefreiheit unterschiedlich beeinflusst: Es gibt Reisende mit hohen Risikoscores, die an den Flughäfen strengeren Kontrollen unterzogen und zuweilen am Reisen gehindert werden. Passagiere hingegen, die als wenig riskant eingestuft werden, müssen weniger strikte Kontrollen über sich ergehen lassen. In diesem Sinne läuft Big Data auf eine Individualisierung von Mobilitätsregeln hinaus.

Daran gibt es jedoch auch Kritik: „Risikopassagiere" werden nicht aufgrund ihrer Identität und nachgewiesener Vergehen, sondern aufgrund eines datenbasierten Risikowerts in ihrem Grundrecht auf Mobilität eingeschränkt. Dies kann leicht dazu führen, dass bestimmte Gruppen unfair behandelt werden. Dabei

haben Reisende wenig Einfluss auf die Daten, anhand derer ihr Risikowert ermittelt wird, und sie können sich entsprechend kaum gegen ihren Score und die damit einhergehende Behandlung wehren. Dies verletzt ihre informationelle Selbstbestimmung und das Recht auf Gleichbehandlung.

Nicht nur Reisende werden durch die PNR-Analysen potenziell in ihren Handlungsmöglichkeiten eingeschränkt, sondern auch die Regelanwender. Diesen verbleiben wegen der mutmaßlich hohen Autorität der Risikoscores vermutlich kaum Freiräume für Ausnahmen. Wie verbindlich die Scores durch Sicherheitsbeamte und Flughafenpersonal gehandhabt werden (müssen), ist allerdings nicht erforscht. Es liegen auch keine Evaluationen dazu vor, ob die PNR-Auswertung die Reisesicherheit erhöht hat und welche Gruppen von Reisenden Vor- und Nachteile erfahren. Wegen Sicherheitsinteressen und den Geschäftsgeheimnissen der Unternehmen ist der Zugang zu den PNR, den Risikoscores und den damit verbundenen Sicherheitsstrategien sehr begrenzt. Dies ist aus demokratietheoretischer Perspektive hoch problematisch.

Big Data kann also, wie in den PNR eingesetzt, als besondere Form der Regulierung genutzt werden. Diese Big-Data-basierte Regulierung zeichnet sich dadurch aus, dass Regeln stärker nach Subgruppen oder gar Individuen differenziert werden. Dies kann die Regulierung prinzipiell effektiver, effizienter und gerechter machen. Es kann aber auch unfair oder gar diskriminierend wirken. Eine weitere Eigenschaft von Big-Data-basierter Regulierung ist, dass die Setzung und die Implementierung von Regeln zusammenfallen. So gibt Big Data anhand der Risikoscores vor, wie ein jeder Passagier behandelt werden muss. Da die Kontrolleure an Flughäfen keinen Einblick in die Entstehung der Scores haben, können sie keine abweichende Entscheidung treffen und sind somit vollständig Vollzugsgehilfen des maschinenbasierten Regulierungssystems. Mit Blick auf eine zuverlässige Umsetzung und die Kosten, die üblicherweise für die Auslegung von Regeln und die Kontrolle von Implementierung anfallen, ist dies positiv.

Problematisch ist jedoch, dass auf diese Weise menschliche Freiheiten eingeschränkt werden: Die Regelanwender (Sicherheitsbeamte, Mitarbeiter von Fluglinien) können keine abweichenden Einzelfallentscheidungen treffen, und die Reisenden haben kaum Möglichkeiten, sich gegen die maschinell erzeugte Empfehlung zu wenden oder diese nachträglich zu beeinflussen.

Eine weitere Besonderheit der beschriebenen Big-Data-basierten Regulierung ist, dass sie wenig transparent ist. Datensätze, Auswertungsverfahren und Entscheidungssysteme sind nur in groben Zügen bekannt. Dieser Mangel an Transparenz räumt den Anwendern große Flexibilität ein, um die Systeme zu handhaben und weiterzuentwickeln. Er ist auch Kern von Geschäftsmodellen und Sicherheitsstrategien. Doch die Kehrseite sind Defizite mit Blick auf öffentliche Kontrolle, Legitimität, Zurechenbarkeit und individuelle Autonomie. Dies schädigt nicht nur die betroffenen Individuen, sondern auch den demokratischen Rechtsstaat.

Angesichts der diskutierten möglichen gesellschaftlichen Schäden von Big Data ist eine weitere Debatte darüber entbrannt, wie Big Data reguliert werden soll. Ein Narrativ dieser Debatte ist, dass Big Data die Regulierung, die wir kennen, grundlegend infrage stellt. So beruhen viele Big-Data-basierte Anwendungen darauf, verschiedene Daten zu verbinden und für immer neue Zwecke zu verwenden. Dies ist mit zentralen Prinzipien des Datenschutzes kaum vereinbar, die besagen, dass personenbezogene Daten nur dann erhoben und verwendet werden können, wenn die Individuen ausdrücklich zugestimmt haben und Daten nur für den eingangs festgelegten Zweck genutzt werden dürfen. In der Folge diagnostizieren Beobachter systematische Defizite in der Durchsetzung datenschutzrechtlicher Regeln und zahlreiche Regulierungslücken. Eine häufig formulierte Erklärung für die Regulierungsdefizite lautet, dass die politische Entwicklung nicht mit der technologischen Schritt halten könne. Doch ein Blick auf die Debatte legt offen, dass es nicht an Regulierungsvorschlägen mangelt. Plausibler ist vielmehr, dass viele Vorschläge ganz unterschiedlicher Ausrichtung miteinander konkurrieren. Dies lässt sich anhand eines Regulierungsvorschlags

Lena Ulbricht ist Wissenschaftlerin in der Projektgruppe Politikfeld Internet. In dem Projekt „Assessing Big Data" forscht sie über Regulierung in der Big-Data-Gesellschaft. *[Foto: David Ausserhofer]*

lena.ulbricht@wzb.eu

Das Big-Data-Projekt

Das vom Bundesministerium für Bildung und Forschung finanzierte Projekt „Assessing Big Data" widmet sich aus multidisziplinärer Perspektive den gesellschaftlichen Implikationen von Big Data. Die Projektgruppe Politikfeld Internet entwickelt einen politikwissenschaftlichen Zugang zum Thema. Weitere Forschungsgruppen in Deutschland blicken aus Perspektive der Ethik, der Soziologie, der Rechts- und der Wirtschaftswissenschaften auf Big Data.

verdeutlichen, der verlangt, Wettbewerbsregulierung für datenschutzpolitische Ziele einzusetzen.

Der Gedanke ist erst einmal überraschend: Wettbewerbsregulierung nimmt Märkte in den Blick und nicht individuelle Freiheits- und Selbstbestimmungsrechte oder den gesellschaftlichen Zusammenhalt. Dass der Ansatz dennoch in den letzten Jahren intensiv debattiert wurde, liegt an seiner Sensibilität für Machtverhältnisse. Befürworter dieses Regulierungsansatzes erhoffen sich eine Antwort auf die (wahrgenommene) Machtkonzentration einiger großer datenverarbeitender Unternehmen, die zulasten der Macht von Verbraucherinnen sowie staatlicher Regulierungs- und Kontrollinstanzen geht. Die monopolartigen Strukturen in der Datenwirtschaft entstehen durch sogenannte Netzwerkeffekte: Je mehr Nutzer vorhanden sind, umso mehr Nutzer (und Anzeigenkunden) können gewonnen werden. Wer beispielsweise einem sozialen Online-Netzwerk beitreten will, wird meistens jenes auswählen, das die meisten Mitglieder hat und somit die größte Reichweite bietet. Haben Unternehmen wie Facebook erst einmal eine Monopolstellung erreicht, können sie Datenschutzstandards senken, ohne befürchten zu müssen, dass ihre Nutzer zur Konkurrenz wechseln. Staatliche Datenschutzkontrollbehörden haben wiederum angesichts der technischen und juristischen Stärke großer Konzerne zu wenig Personal und rechtliche Eingriffsmöglichkeiten, diese effektiv zur Ordnung zu rufen.

Wenn Unternehmen nun ihre Marktmacht zulasten der Nutzerinnen missbrauchen, kann prinzipiell die Wettbewerbsregulierung eingreifen. Dieser Lesart folgend hat das Bundeskartellamt 2016 ein Verfahren gegen Facebook eingeleitet, um dem Verdacht nachzugehen, dass das Unternehmen seine dominante Marktposition dazu nutzt, Nutzer mangelhaft über die Erhebung und Verwendung ihrer persönlichen Daten zu informieren. Die Wettbewerbsaufsicht tritt auch dann auf den Plan, wenn der Wettbewerb zwischen Unternehmen dadurch gefährdet ist, dass manche sich an die geltenden datenschutzrechtlichen Regeln halten und andere nicht. So kritisiert der Wirtschaftswissenschaftler Eric K. Clemons, dass die Vormachtstellung von Google in Europa nicht auf technologischer Überlegenheit, sondern auf dem systematischen Verstoß gegen europäisches Datenschutzrecht beruht. Würden Google und weitere Monopolisten verpflichtet, sich an die Regeln zu halten, hätten auch andere Unternehmen eine Chance, ihre Marktanteile zu erhöhen, etwa jene, die besonders auf Datenschutz und Datensicherheit achten. Dies würde Nutzerinnen wiederum Alternativen und somit einen Autonomiegewinn bieten.

Prinzipiell fordern die Befürworter einer solchen Regulierungsstrategie, dass Wettbewerbsbehörden mit neuen und mehr Kompetenzen ausgestattet werden und stärker mit Datenschutzkontrollbehörden zusammenarbeiten. Für eine solche Verbindung von Wettbewerbs-, Datenschutz- und Verbraucherschutzregulierung treten neben dem Bundeskartellamt auch der Europäische Gerichtshof und der Europäische Datenschutzbeauftragte ein.

Kritikerinnen dieses Vorschlags wie etwa die Generaldirektion Wettbewerb (GD Wettbewerb) der Europäischen Kommission wenden ein, dass Verstöße gegen das Datenschutzrecht durch die Akteure und Instrumente der Datenschutzregulierung bekämpft werden sollten und nicht auf dem Nebenschauplatz der Wettbewerbspolitik. Sie befürchten, dass die Definitionen und Instrumente der Wettbewerbsregulierung ausgeweitet werden müssen, um den Zielen des Daten- und Verbraucherschutzes auf internetbasierten Märkten gerecht zu werden, und sie dadurch grenzen- und substanzlos werden. So orientiert sich Wettbewerbsregulierung bislang daran, ob Monopole Verbrauchern mit Blick auf den Preis und die Qualität von Gütern und Dienstleistungen schaden. In welcher Form der Umgang von Monopolen mit den persönlichen Daten der Kundinnen bewertet werden soll, ist bislang eine offene Frage.

Was ist also Big Data, und was sollte es sein? Big Data ist eine neue Form der gesellschaftlichen Regulierung – mit Vorteilen, aber auch mit Nachteilen. Regeln können gezielter und effizienter eingesetzt werden; die maschinenbasierten Systeme können aber auch menschliche Autonomie verringern. Big Data muss entsprechend selbst auch reguliert werden. Ob die Übermacht großer Unterneh-

men, die sich jahrelang fast ungehindert entwickeln konnten, begrenzt werden kann, hängt auch davon ab, ob ihre Gegner sich zusammenschließen. Datenschützer, Marktwächter und Verbraucherschützer könnten die Rolle übernehmen, die die Gewerkschaften in der industriellen Revolution innehatten. Denn wenn Daten das neue Öl sind, sind Verbraucher und Nutzer die neuen Arbeiter.

Literatur

Amoore, Louise: „Data Derivatives. On the Emergence of a Security Risk Calculus for Our Times". In: Theory, Culture & Society, 2011, Vol. 28, No. 6, pp. 24–43. DOI: 10.1177/0263276411417430.

Clemons, Eric K.: „The EU Files Complaints Against Google, and It's About Time!" In: Huffington Post, 15. April 2015. Online: http://www.huffingtonpost.com/eric-k-clemons/the-eu-files-complaints-against-google_b_7069780.html (Stand 14.08.2016).

European Data Protection Supervisor: Privacy and Competitiveness in the Age of Big Data. The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy. Brussels: EDPS 2014. Online: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf (Stand 16.12.2016).

Ulbricht, Lena/Haunss, Sebastian/Hofmann, Jeanette/Klinger, Ulrike/Passoth, Jan-Hendrik/Pentzold, Christian/Schneider, Ingrid/Strassheim, Holger/Voß, Jan-Peter: „Dimensionen von Big Data: eine politikwissenschaftliche Systematisierung". In: Reinhard Heil/Barbara Kolany-Raiser/Carsten Orwat (Hg.): Big Data und Gesellschaft. Eine multidisziplinäre Annäherung. Wiesbaden: Springer (im Erscheinen).