



Grundsätze für das sozialdemokratische Datenzeitalter

1. Einleitung

Als im Jahr 2005 der frischgewählte Papst Benedikt vorgestellt wurde, blickte die Menschenmasse direkt auf den Balkon des Peterdoms. Acht Jahre später, bei der Vorstellung von Papst Franziskus im Jahr 2013, zeigte sich ein komplett anderes Bild: Die Gesichter waren hinter blinkenden Displays verschwunden. Kaum ein anderes Bild stellt so gut dar, wie die digitale Kommunikation unsere Welt verändert hat.

Dank Smartphones, Laptops, Smart Homes und sozialen Netzwerken befinden wir uns derzeit auf der Schwelle von der Small-Data- in die Big-Data-Welt. Daten erfüllen schon heute eine wichtige gesellschaftliche Funktion. So bestehen die Wissenschaften zum großen Teil daraus, Daten zu sammeln, sie auszuwerten und daraus Schlüsse für uns alle zu ziehen. Klimaforscher*innen fahren beispielsweise zum Polarkreis, um Daten aus dem Eis zu sammeln. Wir nutzen Daten schon lange, um unsere Welt besser zu verstehen.

Dann kam die Revolution hin zu Big Data. Es handelt sich hierbei um eine Umwälzung, von der jede*r Einzelne betroffen ist. Künftig werden wir uns dem Einfluss der Daten und ihrer

Auswertung nicht mehr entziehen können. Umso wichtiger ist es, dass die Sozialdemokratie endlich anfängt zu verstehen, welche Umbrüche sich derzeit vollziehen.

Moderne und künftig absehbare Möglichkeiten zur Datengenerierung und -nutzung bergen noch immer ungeahnte Chancen für gesellschaftlichen und wirtschaftlichen Fortschritt. Im Bereich der Gesundheit können sie zum Beispiel dazu beitragen, Krebs dauerhaft zu besiegen, im Bereich der Mobilität können Verkehrsstaus minimiert werden und im Bereich der Energie können sie zur effizienten Stromverteilung und -management beitragen. Zugleich bergen diese Möglichkeiten auch neue Risiken der Manipulation, der Diskriminierung und der Schaffung neuer sozialer Ungleichheit. Wir Sozialdemokrat*innen sind gefordert, die Chance zu nutzen den Wohlstand für alle zu mehrern und zugleich die Risiken neuer Ausgrenzung zu minimieren. Wir stellen ernüchtert fest, dass mit der bisherigen Datenpolitik beide Ziele vermutlich verfehlt werden.

Die SPD muss die Partei der sozialen Gerechtigkeit und der selbstbestimmten sozialen Teilhabe des digitalen Zeitalters werden. In Zeiten, in denen sich Wirtschaftsbereiche auflösen und neue soziale, politische und wirtschaftliche Herausforderungen entstehen, reicht es in vielen Fällen nicht aus, einzelne Regeln punktuell anzupassen, sondern wir müssen unsere sozialdemokratischen Werte grundsätzlich neu übersetzen. Freiheit, Gerechtigkeit und Solidarität sind im digitalen Zeitalter genauso wichtig und aktuell wie im Industriezeitalter, aber die Themen, Herausforderungen und Antworten sind neu. Sie sind darüber hinaus derzeit vielfältig und aufgrund des schnellen Wandels so schwer vorhersehbar, dass es wichtig ist, neue Regeln zu etablieren, die die wesentlichen Pflöcke frühzeitig einschlagen.

Dreh- und Angelpunkt hierfür ist eine moderne Datenpolitik. Sie stellt, in einem weiten Sinne gefasst, das Fundament der Gesellschaftspolitik des 21. Jahrhunderts dar. Sie muss nicht nur festlegen, welche Daten Staat, Wirtschaft und Wissenschaft verarbeiten dürfen, sondern künftig auch welche Konsequenzen sie aus den Daten ziehen dürfen, also wo es erlaubt ist, Unterschiede zwischen Menschen zu machen, und wo nicht. Wichtig dabei ist: Weder können wir uns gegen den wirtschaftlichen Fortschritt stellen, noch dürfen wir dem Kapital das Feld alleine überlassen. Wenn wir bestehende Regulierung in Teilen nicht auf den Prüfstand stellen, riskieren wir die gesellschaftliche und wirtschaftliche Entwicklung großen

internationalen Konzernen zu überlassen; wenn wir neue Risiken nicht mitdenken und frühzeitig regulieren, riskieren wir Deutschland dem Turbokapitalismus preiszugeben.

Mit dem Big-Data-Zeitalter folgt also eine neue Gerechtigkeitsfrage: Wer kontrolliert meine Daten? Unter welchen Bedingungen habe ich Zugang zu Informationen und gesellschaftlicher Teilhabe in Zeiten zunehmender Digitalisierung des Lebens? Dabei handelt es sich im Kern um Gerechtigkeits- und Verteilungsfragen. Es geht um die Kontrolle und die Modalitäten der Nutzung von Daten. Es geht um soziale Teilhabe und Partizipation. Diese Erkenntnis ist zentral für uns. Denn das heißt, dass wir diese Fragen ins Zentrum unserer Politik rücken müssen. Ziel dieses Papiers ist es daher, die notwendigen Korrekturen bei der weiteren Entwicklung der digitalen (Netz-) Welt anzustoßen. Wir haben keinen Anspruch auf Vollständigkeit, bei einem so großen Feld kann man nicht alle Bereiche abdecken. Dieses Papier ist als Denkanstoß gedacht der dann hoffentlich zu einer breiten Debatte über das sozialdemokratische Datenzeitalter führen wird.

2. Fehlleitungen derzeitiger Datenpolitik

Die derzeitige Datenpolitik krankt daran, dass sie sich nahezu sklavisch allein an den Datenschutzprinzipien des 20. Jahrhunderts orientiert. Auf diese Weise lässt sie wesentliche Entwicklungen der Digitalisierung systematisch außer Acht: Sie blendet die Attraktivität von mit Datenverarbeitung zusammenhängenden Dienstleistungen aus, negiert die Relevanz von – auch personenbezogenen – Daten für die gesellschaftliche und wirtschaftliche Weiterentwicklung und adressiert zugleich die eigentlichen Risiken des digitalen Zeitalters für die Bürger*innenrechte nur unzureichend. Durch die Datenschutzgrundverordnung haben wir erstmals einen gemeinsamen europäischen Rechtsrahmen. Dies gilt es ausdrücklich zu begrüßen. Doch trotz vieler guter Punkte innerhalb der Datenschutzgrundverordnung, wie z.B. den hohen Sanktionsmöglichkeiten, sehen wir die Gefahr, dass sie viele Fehlentwicklungen nicht wird verhindern können, hingegen mitunter viele neue Innovationen und datengetriebene Geschäftsmodelle in Europa verhindern könnte, die dann am Ende durch US-amerikanische Unternehmen mit einem anderen Datenschutzverständnis gestaltet werden.

- Die Attraktivität von Datenangeboten

Auf die Kundin oder den Kunden maßgeschneiderte Angebote sind die konsequente Weiterentwicklung der Dienstleistungsgesellschaft. Die Folge ist, dass große Unternehmen mit einem vollumfänglichen Leistungsangebot durch die Datenschutzgrundverordnung profitieren, da sie aufgrund ihres Geschäftsmodells mehr Daten über ihre Kund*innen erheben können. Dies führt dazu, dass wenige große Player besser maßgeschneiderte Services anbieten können. Denn eines der wesentlichen Erfolgsfaktoren künftigen privatwirtschaftlichen Erfolges wird sein, den Kund*innen für jeden Moment die beste individuelle Dienstleistung zu bieten. Nur die Firmen, die die Bedürfnisse ihrer Kund*innen kennen, werden in wenigen Jahrzehnten am Markt bestehen können. Sich diesem globalen Digitalisierungstrend entgegenzustellen würde bedeuten, sich als Deutschland und Europa wirtschaftlich und gesellschaftlich von neuen Services quasi abkoppeln zu wollen. Es würde zudem bedeuten, Dienstleistungen, die sich hoher Beliebtheit erfreuen, quasi zu verbieten.

- Unklar: Bekenntnis zu Big-Data-Analysen mit personenbezogenen Daten ja oder nein?

Die Zweckbindung in der Datenschutzgrundverordnung in ihrem heutigen Zustand muss weiterentwickelt werden. Big-Data-Analysen bieten große Chancen in vielen Gebieten, indem gesellschaftliche, biologische und prozessurale Zusammenhänge von Computern entdeckt werden, die mit herkömmlichen Methoden und kleinen Datenbanken nicht gefunden werden können. Es ist bislang rechtlich unklar, ob eine Pseudonymisierung zu deren Verarbeitung berechtigen würde. Für Unternehmen und Wissenschaft werden somit nicht nur Barrieren zur kommerziellen Verwertung von personenbezogenen Daten geschaffen, sondern auch zur Entdeckung neuer Zusammenhänge, die die Gesellschaft und die Menschheit voranbringen können. Damit wird in der deutschen Wirtschaft und Wissenschaft weitere Unsicherheit geschaffen. Im Endeffekt machen wir uns hierdurch noch einen Schritt weiter abhängig von US-Unternehmen, die von dieser Regelung profitieren werden. Im Gegensatz zu deutschen Forschungseinrichtungen und kleinen europäischen Start-Ups können die großen amerikanischen Unternehmen sehr schnell auf rechtliche Unsicherheiten reagieren. Die guten Absichten der neuen europäischen Datenregulierung drohen vor allem zu einer großen Rechtsunsicherheit zu führen, die

in erster Linie der europäischen Wissenschaft und den kleinen Unternehmen schadet.

In der Summe sind alle Datenschutzprinzipien darauf ausgerichtet, welche Daten überhaupt erhoben sowie wie lange diese gespeichert und verarbeitet werden dürfen. Wenn es sich dabei zudem um Unternehmen außerhalb Europas handelt, die auch Daten außerhalb Europas speichern, ist fraglich, ob der europäische Datenschutz dort wirklich wirksam greift. Deshalb gilt es, sich intensiv über regulative Maßnahmen Gedanken zu machen, die Fehlentwicklungen bei aufgrund von Big-Data-Analysen gezogenen Schlussfolgerungen und Entscheidungen verhindern.

3. Wie eine sozialdemokratische Datenpolitik gestaltet werden kann

Neben der Problematik der Regulierung der Erhebung von Daten krankt die derzeitige Politik auch daran, dass die politische Regulierung immer langsamer ist als die technologische Entwicklung. Demokratische Entscheidungen brauchen nun mal (glücklicherweise) ihre Zeit und sollen ja auch breit diskutiert werden. Egal wie schnell die Politik handelt, wir werden immer der Technik hinterherlaufen und beim Versuch der Regulierung scheitern. Daher wollen wir in diesem Papier einen anderen Weg vorschlagen. Anstatt auf jede neue technische Entwicklung mit einer neuen Regulierung zu reagieren, wollen wir in diesem Papier politische Prinzipien in der Datenpolitik aufstellen. Diese Prinzipien sollen die Grundpfeiler einer neuen sozialdemokratischen Datenpolitik darstellen und können dann schnell auf neue technologische Umbrüche angewendet werden. Durch diese Prinzipien haben sowohl die Politik als auch die Unternehmen und die Nutzer*innen klare und langfristige Regularien, an denen sie sich orientieren können. Die große rechtliche Unsicherheit auf allen Seiten würde wegfallen.

Für nachfolgende Prinzipien gilt es somit, konzeptionelle und technische Umsetzungswege zu finden. Für einige können wir bereits erste konkrete Lösungswege beschreiben, bei anderen müssen wir jetzt schnell politische Umsetzungsmöglichkeiten erarbeiten.

Grundsatz Nr. 1 – Die Nutzungshoheit über Daten zurückerlangen!

Der Grundsatz der reinen Datenvermeidung ist für uns überholt. Durch reine Datenvermeidung werden wir vom sozialen Leben oft ausgeschlossen und viele Dienste machen erst Sinn und Spaß, wenn sie mit eigenen Daten angereichert werden. Schaut man sich die erfolgreichsten Apps und sozialen Netzwerke an, dann sind dies meist sogenannte Datenkraken. Mit diesem Faktum müssen wir politisch umgehen. Anstatt an einer Regelung des 20. Jahrhunderts festzuhalten und damit immer wieder zu scheitern, muss sich die Politik den neuen Gegebenheiten anpassen. Die Selbstbestimmung über eigene Daten ist im Gegensatz zur reinen Datenvermeidung notwendiger denn je. Es gibt gute Gründe, warum Menschen ihr persönliches Leben ein Stück weit öffentlich darstellen wollen und warum sie deshalb Unternehmen Daten geben. Es gibt aber auf der anderen Seite auch sehr gute Gründe, die eigenen Daten vor Staat und Unternehmen zu schützen. Von der Selbstbestimmung über die eigenen Daten entfernen wir uns politisch aber immer weiter. Kaum ein*e Nutzer*in weiß, welche Daten über sie/ihn überhaupt erhoben werden oder wem die Daten dann wirklich „gehören“. Für uns gilt: Der/die Nutzer*in muss die Entscheidungshoheit über die Verwendung von seinen/ihren Daten behalten.

Lösungswege

So einfach sich dieser Ansatz politisch anhört, so schwierig ist er praktisch umzusetzen. Und doch gibt es einiges, was die Politik machen kann. So brauchen wir bei der Verarbeitung und Erhebung von Daten endlich eine wirkliche Transparenz. Die Unternehmen müssen verpflichtet werden, den Nutzer*innen eine Rückmeldung zu geben, welche Daten erhoben werden und was sie mit diesen machen. Und das auf eine Art und Weise, die die/der Nutzer*in auch versteht. Einige Unternehmen sind hierbei schon vorangegangen und stellen sämtliche Aktivitäten (geräteübergreifende Browserhistorie, Bewegungsdaten, Nutzung von Apps, etc.) für die Nutzer*innen in nachvollziehbarer Art und Weise dar. Zudem lassen sich dort sämtliche Aktivitäten, aber auch jede einzelne Aktivität individuell löschen. So lassen sich insbesondere für den einzelnen Menschen heikle Daten sofort beseitigen. Ein solches Vorgehen muss verbindlich für alle Unternehmen festgelegt werden. Wir begrüßen, dass die EU-Datenschutzgrundverordnung genau diesen Weg beschreitet.

Grundsatz 2 - Dezentralität von Daten und Akteursvielfalt

Ein wichtiger Grundsatz des Internets sollte seine technische Dezentralität und seine Akteursvielfalt. Es gibt kein Zentrum im Internet, sondern nur Datenknoten, die miteinander verbunden sind. Dies ist wohl das wichtigste infrastrukturelle Merkmal des Internets. Es erklärt auch, warum das Netz so schnell so erfolgreich wurde und warum es diesen großen gesellschaftlichen Wandel mit sich gebracht hat.

Bis vor wenigen Jahren war es auch so, dass unsere Daten bei sehr unterschiedlichen Unternehmen und Servern gespeichert waren. Es gab einfach viele kleinere Unternehmen und so war die Gefahr des Datenmissbrauchs recht gering. Im letzten Jahrzehnt hat sich das grundlegend gewandelt. Heute dominieren wenige große US-amerikanische Unternehmen viele Lebensbereiche und damit auch unsere Daten. Dienstleister wie Facebook und Google versuchen zudem immer stärker ein geschlossenes System im Internet zu werden. Diese Bestrebungen greifen die grundlegenden Prinzipien des Internets an. Auch für den Datenschutz hat diese Entwicklung schwerwiegende Folgen.

Lösungswege

Wir fordern daher, dass die Dezentralität von Daten wieder gefördert wird. Dies liegt natürlich auf der einen Seite bei den Nutzer*innen selbst. Auf der anderen Seite muss aber auch klar sein, dass Apps und Produkte im selben Unternehmen keinen Datenaustausch betreiben dürfen. So müssen wir zum Beispiel aktuell verhindern, dass WhatsApp seine Nutzer*innendaten einfach an Facebook weitergeben darf. Diese Netzwerkeffekte müssen auch bei der Verschärfung des Wettbewerbsrecht ihren Niederschlag finden. Durch sich immer wieder bildende Datenmonopole ist ein fairer Wettbewerb sonst nicht mehr möglich. Außerdem brauchen wir eine deutlich bessere Infrastruktur für europäische Start-Ups.

Grundsatz 3 - Solidarsysteme behalten

Eine große Errungenschaft, für die die Sozialdemokratie lange gekämpft hat, sind unsere gesellschaftlichen Solidarsysteme. Hierzu zählt sicherlich unsere universelle Krankenversicherung oder das Rentensystem. Egal welche Vorbedingungen jemand mitbringt, egal wie der eigene Lebenswandel aussieht, krankenversichert oder

rentenversichert wird jede*r. Dieses zentrale und solidarische Prinzip haben Datenbewertungen in den letzten Jahren von vielen unbemerkt immer mehr aufgeweicht. Apps und Fitnessarmbänder können zunehmend unsere Ernährung und Bewegung tracken.

Lösungswege

Während es jedem Menschen frei steht, sein oder ihr eigenes Ernährungs- und Bewegungsverhalten zu dokumentieren, muss klar definiert werden, inwiefern Staat, Krankenkassen oder privaten Krankenversicherungen, diese Daten nutzen dürfen. Das Solidarsystem darf an dieser Stelle unter keinen Umständen ausgehöhlt werden. Zugleich setzen wir uns dafür ein, dass Wissenschaft und Forschung ein hochgesicherter Bereich bereit gestellt wird, in dem Daten aus dem Gesundheitssystem von sich hierzu bereit erklärenden Patient*innen ausgewertet werden können. Aufgrund der Sensibilität dieser Daten soll für ein derartiges System die Expertise aus allen gesellschaftlichen Bereichen zusammengetragen werden.

Grundsatz 4 – Soziale Diskriminierung durch Algorithmen verhindern

In Zukunft werden immer mehr Entscheidungen getroffen, die nicht nur auf digital erhobenen Daten, sondern auf Algorithmen basieren. Diese werden immer weniger allein durch Menschenhand erstellt, sondern entwickeln sich durch machine-learning selbstständig weiter. Hierbei werden, vereinfacht gesagt, aufgrund von Beobachtungen Zusammenhänge zwischen Individuen mit ähnlichen Eigenschaften ermittelt. Zusammen mit vielen weiteren Variablen können oft bereits sehr detaillierte Schlussfolgerungen gezogen werden – auf ihnen basierte Entscheidungen werden täglich millionenfach im Internet getroffen. Dabei basieren diese stets auf statistischen Wahrscheinlichkeiten und niemals auf 100-prozentig gesicherten Kausalitäten. Dies ist nicht grundsätzlich zu kritisieren, auch menschliche Entscheidungen basieren selten auf 100-prozentig sicheren Erkenntnissen, oftmals verstecken sich in diesen mindestens ebenso subjektive, gesellschaftlich nicht wünschenswerte Vorurteile.

Datenvorhersagen sind daher grundsätzlich nichts Verwerfliches. Bei der Datenvorhersage von Naturkatastrophen beispielsweise können Vorhersagen viele Menschenleben retten.

Uns muss aber klarwerden, dass Vorhersagen nur Prognosen sind und Prognosen können daher auch falsch sein.

Lösungswege

Wir brauchen eine hohe Transparenz bei Vorhersagen, konkret: auf welchen Annahmen beruhen diese und welche Daten wurden hierzu benutzt? Denn erst diese Transparenz liefert uns auch die Möglichkeit der Widerlegbarkeit von Handlungsvorhersagen.

Wichtige und vor allem bindende Entscheidungen dürfen zudem nicht alleine von Maschinen und Algorithmen getroffen werden, sondern hier muss auch noch ein Mensch einen zweiten Blick auf die Daten werfen, analog dem 4-Augen-Prinzip. Außerdem ist es wichtig, dass wir durch Datenbewertungen nicht zu einer neuen diskriminierenden Bewertungsgesellschaft führen. Technische Infrastruktur ist auch immer politisch. Daher müssen wir hier bereits beim Programmieren der Software ansetzen.

Aufgrund der bislang nicht abzuschätzenden Wirkung von künstlicher Intelligenz auf die Gesellschaft sollten wir darüber nachdenken, ob im Rahmen der Technikfolgenabschätzung (TA) nicht verstärkt auch der digitale Bereich mit in die Risikobetrachtung einbezogen werden sollte. Angesichts des in den kommenden Jahren verstärkten Einsatzes von „disruptive technologies“ ist es auch notwendig, eine digitale Ethik einzuführen, um den Missbrauch von Algorithmen zu verhindern.

Grundsatz 5 – Das Wissen über Daten erhöhen

Ein großes Problem jeglichen Versuches der Regulierung von Datennutzung ist der Informationsgap über das Wissen bezüglich Daten innerhalb der Nutzer*innen. Während die einen wissen, welche Daten über sie erhoben werden, und in der Lage sind, ihre Daten zu verschlüsseln, hat sich ein Großteil der Nutzer*innen noch nie mit dem Thema Datennutzung auseinandergesetzt. Obwohl die Datennutzung einer der großen zukünftigen gesellschaftlichen Fragen sein wird, gibt es für die/den einzelne*n Nutzer*in kaum Möglichkeiten, bei dem Themenfeld mehr Wissen zu erlangen.

Lösungswege

Wir fordern daher eine verstärkte staatliche Anstrengung, den Informationsgap bei dem Thema Daten innerhalb der Bevölkerung zu verkleinern – als Teil einer umfassenden Stärkung der Medienkompetenz. Der Umgang mit Daten gehört daher in die Lehrpläne der Schulen. Die vielen ehrenamtlichen Initiativen, die es in diesem Bereich gibt, sollen zukünftig eine verstärkte staatliche Unterstützung erhalten. Außerdem müssen Unternehmen in die Pflicht genommen werden, die Transparenz im Umgang mit Daten zu erhöhen, um den Nutzer*innen entgegenzukommen.

Grundsatz 6 – Für mehr Sicherheit: Fokus auf wirksame Ermittlungsarbeit und nicht den Datenheuhaufen

Ein Eingriff in die digitale Privatsphäre ist nicht so eindrucksvoll wie eine Hausdurchsuchung. Chatprotokolle, Fotos und Surfverhalten sind aber genau so intim. In den vergangenen Jahren haben wir die Sicherheits- und Überwachungsgesetze immer weiter verschärft. Mehrere Überwachungsmaßnahmen wurden beschlossen, die Vorratsdatenspeicherung eingeführt. Die Eingriffs- und Überwachungsmöglichkeiten des Staates wurden immer weiter ausgebaut – mit zweifelhaftem Erfolg für unsere Sicherheit.

Wir stellen grundsätzlich infrage, dass mehr Daten und mehr Überwachung auch wirklich zu mehr Sicherheit führen. Es gibt derzeit keine Hinweise dafür, dass die Suche nach der Nadel im Heuhaufen einfacher wird, indem man den Heuhaufen immer weiter vergrößert. Im Gegenteil: Selbst in den Sicherheitsbehörden westlicher Staaten gibt es viele hochrangige Skeptiker*innen, die es für verfehlt erachten, sich auf Investitionen in Server, Software und Datenanalysen zu verlassen, und die die hierfür aufgewendeten Mittel lieber für einen Personalausbau in den Bereichen bewährter und effektiver Ermittlungsmethoden verwenden würden. Es wird daher Zeit für eine rationale Sicherheitspolitik, die bereit ist, kritisch zu evaluieren, welche Maßnahmen wirklich die Sicherheit erhöhen – und die nicht aktionistisch immer nur mehr Überwachung fordert. Außerdem gilt es, kritisch zu prüfen, wo die Zusammenarbeit zwischen Geheimdiensten und polizeilichen Behörden gerechtfertigt ist.

Lösungswege

Wir fordern eine grundsätzliche Prüfung, welche Maßnahmen tatsächlich Wirkung zeigen. Dann gilt es, mit kühlem Kopf zwischen Wirksamkeit, Grundrechtseingriff und Missbrauchspotenzial abzuwägen. Dabei sind wir nicht dogmatisch: wo es einen wirklichen Verdacht gibt, soll es auch möglich sein, eine/n Verdächtige*n zu überwachen. Eine grundsätzliche Überwachung aller Bürger*innen, wie es die Vorratsdatenspeicherung vorsieht, kann aber niemals verhältnismäßig sein. Deswegen fordern wir die sofortige Abschaffung dieser Überwachungsmaßnahme und setzen uns gegen jegliche Form der verdachtsunabhängigen Überwachung ein.

Ein großer Teil der staatlichen Überwachung erfolgt nicht über die polizeilichen Behörden, sondern über die Geheimdienste. Die Enthüllungen von Edward Snowden haben gezeigt, in welchem Umfang die Geheimdienste ohne rechtliche Grundlage unsere gesamte Kommunikation überwachen. Die SPD muss zukünftig alle Mittel einsetzen, um ein solches Vorgehen zu unterbinden. International müssen wir deutlich mehr Druck auf die USA und andere Länder in diesem Bereich ausüben. Allerdings müssen wir zunächst den eigenen Hof kehren. Wenn die Bundeskanzlerin sagt: „Ausspähen unter Freunden, das geht gar nicht“, dann müssen daraus auch politische Taten folgen.

Beim eigenen Auslandsgeheimdienst, dem BND, muss die parlamentarische Kontrolle deutlich ausgebaut werden. So brauchen die Abgeordneten deutlich mehr Personal, mehr Zugangsberechtigungen und auch eine Budgetmitsprache. Ohne diese Befugnisse kann es für uns keine wirkliche Kontrolle des Geheimdienstes geben. Das vor kurzem durch die große Koalition verabschiedete BND-Gesetz greift hier zu kurz und muss nachgebessert werden. Außerdem müssen wir deutlich mehr als bislang in die staatliche IT-Sicherheit investieren.

Grundsatz 7 - Open Data Love

Open Data bezeichnet die freie Verfügbar- und Nutzbarkeit von öffentlichen, nicht personenbezogenen Daten. Open Data gehört für uns zu einem guten und transparenten Regieren dazu. Es sollte absoluter Standard sein, dass der Staat seine Daten automatisch freigibt. Wir fordern daher einen Rechtsanspruch auf offene Daten. Die Daten gehören den Bürger*innen, die mit ihren Steuern dafür gesorgt haben, dass der Staat sie erheben kann.

Lösungswege

Das Open-Data-Gesetz muss daher verpflichtend vorschreiben, dass alle Daten, deren Veröffentlichung nicht ein anderes Gesetz entgegenpricht, auch der Öffentlichkeit unter einer freien Lizenz und maschinenlesbar zur Verfügung gestellt werden müssen. Die digitalen „Schätze“ des öffentlichen Sektors müssen gehoben werden und zu einer Verbesserung der Gesellschaft mitbeitragen. Zusätzlich können offene Daten auch dazu führen, dass sich neue Unternehmen gründen. Die Hauptherausforderung liegt hier allerdings nicht bei der Regulierung. Viel wichtiger als diese ist die Ausstattung der Behörden mit Personal und Expertise zur Veröffentlichung der Daten. Wir fordern daher die verpflichtende Einrichtung einer Open-Data-Stelle in jedem Ressort. Auf jede tausendste vollzeitäquivalente Personalstelle muss diese mit mindestens einer Vollzeitstelle ausgestattet werden, die bei der konzeptionellen und technischen Offenlegung unterstützt. Wünschenswert ist die Öffnung von Schnittstellen zu Sensoren, die zur Steuerung der Stadt zukünftig genutzt werden.