



Mittwoch, 24. Juli 2019, 15:00 Uhr
~18 Minuten Lesezeit

Die gläserne Gesellschaft

Die Debatte um informationelle Selbstbestimmung und Datensicherheit betrifft uns alle.

von Manova Jugendredaktion
Foto: aslysun/Shutterstock.com

„Du musst nicht einmal etwas eintippen. Wir wissen, wo du bist. Wir wissen, wo du warst. Wir können mehr

oder weniger wissen, was du denkst“, äußerte im Oktober 2010 Googles damaliger Geschäftsführer Eric Schmidt beim Second Annual Washington Ideas Forum (1). Diese für alle Verteidiger von Datensicherheit und informationeller Selbstbestimmung erschreckenden Worte verpufften jedoch ebenso wie die vier Jahre darauf folgenden Enthüllungen Edward Snowdens zu NSA-Praktiken im Bereich der Datenüberwachung und Datensammlung. Die Strukturen und Interessen scheinen sich seitdem nicht verändert zu haben. Der medialen Empörung folgte die fragwürdige Fortsetzung der Datenanhäufung – bis heute. Damit scheint es ein offenes Geheimnis, dass Unternehmen persönliche Daten von Nutzern speichern und kommerzialisieren. Aber wieso soll das verkehrt sein – Datensammeln als Ziel einer Gesellschaft? Profitiert der Mensch etwa nicht von höchst individualisierten Angeboten, die ihm zur Verfügung gestellt werden?

von Sasha Stern

In Zukunft wird es für den Menschen sogar noch bequemer. Dank dem Internet der Dinge sollen Computer möglichst unsichtbar in das alltägliche Leben integriert werden. Mark Weiser, der diese Idee erstmals erwähnte, fantasierte in einem Aufsatz aus dem Jahr 1991 über hilfreiche Technologien, die sich im Alltagsgewebe nicht mehr als solche erkennen lassen. Damals gab es, wohlgemerkt, die Möglichkeiten von drahtlosem Netzwerk noch gar nicht.

Heutzutage ist die Rede von Ambient-Assisted-Living, also einem Haushalt, der über Vorräte im Kühlschrank bestimmt und sowohl

Geräusche als auch Laufwege zur Effizienzsteigerung weiterer Geräte aufzeichnet. Dass hierbei sehr private Daten erhoben werden, die schließlich nicht nur der Technologie, sondern auch dem Hersteller und somit Dritten zur Verfügung stehen, wird in der öffentlichen Darstellung selten erwähnt (2, 3).

Mit all den stark beworbenen technischen Zusatzmodulen wie Fitnessarmbändern, Kundenkarten, Smart-TV, Smartphone und unzähligen weiteren Diensten im Internet, zwingt sich der Bürger in ein gläsernes Selbst. Fraglich ist jedoch, welche Gefährdung von der zunehmenden Datensammlung für die Autonomie des Einzelnen ausgeht. Hinzu kommt die Kontroverse, inwieweit an einer Vernetzung des Alltags festzuhalten ist oder ob sich der Mensch damit sogar freiwillig in ein panoptisches Gefüge begibt – dazu später mehr. Bei diesen Leitfragen gilt es, keinen Skeptizismus zu streuen oder Panikmache zu betreiben, sondern durch eine hohe Vielfalt an fundierten Ausarbeitungen und wissenschaftlichen Stimmen aussagekräftige Kritik festzuhalten.

Technologie und Freiheit

Ein gleichnamiges Kapitel findet sich im Essay *Die Industrielle Gesellschaft und ihre Zukunft* von Theodor Kaczynski, das die Washington Post und die New York Times erstmals am 19. September 1995 abdruckten. Kaczynski – Mathegenie, Harvardabsolvent, Mathematikprofessor und Bombenattentäter – verschaffte sich in der Öffentlichkeit Gehör durch selbstgebaute Bomben, mit denen er im Zeitraum von 1978 bis 1995 drei technikaffine Menschen tötete und 23 weitere verletzte. In seinem Manifest rief er zum Widerstand gegen die zunehmende Technisierung der Gesellschaft auf.

Sein Gedankengang bezüglich Einzelinnovationen stellt für diesen

Artikel einen nennenswerten Ansatz dar: Kaczynski zufolge scheinen Erfindungen wünschenswert, wenn sie einzeln betrachtet werden. Beispielhaft sind Elektrizität, motorisierte Fortbewegung und schnelle Kommunikationsmittel zu nennen (4, 5). Er schlussfolgerte zutreffend: „Wie könnte man diese Dinge oder andere der unzähligen technischen Fortschritte ablehnen, die die moderne Gesellschaft entstehen ließ“ (6)?

Somit präzisiert diese Aussage nochmals den Ausgangspunkt dieses Artikels. Denn es existieren unfassbar viele Entwicklungen, die seit dem Ende des 20. Jahrhunderts fortlaufend verknüpft und per Internet vernetzt werden. Infolgedessen entstehen Interdependenzen auf technischer, gesellschaftlicher und soziobiologischer Ebene, die auf eine enorm komplexe Art und Weise zusammenwirken. Das tägliche Leben ist von vielen dieser Faktoren betroffen, wodurch ein Diskurs oftmals schwerfällt, weil es an Distanz und an Objektivität mangelt. Dennoch oder gerade deshalb wird dieser Versuch der Auseinandersetzung im Folgenden unternommen.

Sammlung und Verwendung von Daten

Der Ursprung aller Debatten um Datensammlung und Datensicherheit liegt im Verhältnis der beiden Sphären des Privaten und des Öffentlichen. Es dient als Grundpfeiler moderner Regierungssysteme, eine private Sphäre zu etablieren, einen Raum mit dem „Recht, in Ruhe gelassen zu werden“ (7), in dem sich der Einzelne zurückziehen, informieren und Gedanken fernab staatlicher sowie gesellschaftlicher Einflüsse und Kontrollmechanismen machen kann. Hinzu kommen der Austausch und die Organisation mit anderen Einzelindividuen.

Das Prinzip des Privaten ist im Grundgesetz – der „Verfassung der

Deutschen“ – in Artikel 2 Absatz 2 als Unverletzlichkeit der Person und in Artikel 13 Absatz 1 als Unverletzlichkeit der Wohnung geregelt. In der Europäischen Menschenrechtskonvention lautet es konkret: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“ (8). Damit wird sowohl ein physischer als auch psychischer Raum gewährleistet, frei von Überwachung. Einbezogen ist darin nicht nur das passive „Recht, in Ruhe gelassen zu werden“ (9), sondern auch das Recht auf die Kontrolle persönlicher aus- und eingehender Kommunikationsdaten.

Informationelle Selbstbestimmung stellt somit einen essentiellen Teil individueller Persönlichkeit dar und gilt bisher in demokratischen Gesellschaftsordnungen als fundamentale Errungenschaft (10).

Inzwischen wird der Alltag von allen nur erdenklichen Internetanwendungen bestimmt und infolgedessen findet in einigen Teilen der Welt, vornehmlich auf der Nordhalbkugel, eine Zuspitzung der Kontroverse um Datensicherheit statt. Egal, ob Smartphone, Online-Kauf, Smart-Home-Assistent – beispielsweise Alexa-Sprachsteuerung –, Fitnessarmband oder unterwegs mit einer Suchmaschine: Überall entstehen Spuren wie bei einem Strandspaziergang. Nur mit dem Unterschied, dass es keine Instanz gibt, die wie das Meer die Spuren einfach wieder hinwegspült.

Nach Rainer Kuhlen lassen sich digitale Fußabdrücke in drei Kategorien einteilen. *Distributionsdaten* entstehen durch 1:1- oder 1:n-Kommunikation, wie es beispielsweise per E-Mail oder in Foren, Chats und sozialen Netzwerken der Fall ist. Diese Daten beinhalten formale Angaben zum Sender, Empfänger, Datum oder Gegenstand und können durch Sicherheitsbehörden sogar inhaltlich ausgewertet werden. Weiterhin entstehen sogenannte *Interaktionsdaten* durch Nutzung von Internetdiensten, die grundsätzlich den jeweiligen Betreibern zur Verfügung stehen. Aber

auch Internetanbieter, Suchmaschinen und Auktionshäuser haben Zugang. Schließlich gibt es noch *Transaktionsdaten*, die bei jeglichen Online-Käufen erhoben werden (11).

Bereits beim Starten einer Suchmaschine wie Google gibt man beispielsweise Auskunft über seinen Standort durch die mitgesendete IP-Adresse. Über diese können zudem erneute Anfragen und Aktivitäten ausgewertet und zusammengeführt werden. Dazu zählen beispielhaft Käufe, häufig aufgerufene Internetangebote oder die Nutzungsdauer bestimmter Inhalte. Entsprechend kann aus Einzelinformationen ein ganzes Puzzle, sozusagen ein Persönlichkeitsprofil, erstellt werden (12).

Auf diese virtuellen Identitäten können künftige Angebote ausgerichtet werden. Das kann digital geschehen, wie beispielsweise durch Werbefenster/-banner, personalisierte Angebote, Spam-Mails – oder auch analog, etwa durch personalisierte Post, angebotsorientierte Zusendungen, wenn die virtuelle Identität über die Eingabe von Adressinformationen einer realen Persönlichkeit zugeordnet werden kann. Hinzu kommen Cookies, die bei jeder Suchanfrage im Browser implementiert werden und das allgemeine Verhalten des Anwenders im Internet aufzeichnen. Das Auslesen der Cookies kann hilfreiche Informationen zu einer Profilerstellung generieren. Die dadurch entstehenden Interessenprofile werden oftmals zu Profilen von Interessensgruppen zusammengeschlossen. Dadurch sind Werbezwecke effizienter realisierbar (13, 14).

Mit gegenwärtigen Methoden der Datenerhebung und anschließender Verknüpfung scheint es demnach möglich, eine virtuelle Identität von jedem Nutzer zu erstellen. Das angelegte Profil kann Auskunft zu Interessen durch Käufe und zu häufig aufgerufenen Internetdienste geben.

Da die Fusion persönlicher Daten allerdings nicht nach der

Browseranalyse endet, sondern sich über alle Anwendungsgeräte erstreckt, die mit dem Internet verbunden sind, folgt ein kaum einsehbares Sammelsurium an Persönlichkeitsangaben. Die Kombination gesammelter Daten kann folglich ein vermutlich lückenloses Bild zu Verhalten und Bewegung einer Person erstellen.

Dass die erstellten Profile nicht dazu genutzt werden, um uns eine nachhaltig freundliche Umgebung im Netz zu verschaffen, gründet im vorrangigen Ziel der Gewinnmaximierung vieler Konzerne. Die Philosophin Shoshana Zuboff spricht sogar von einer extremen Form des Überwachungskapitalismus. Denn aus Daten, die Auskunft über individuelle Gedanken, Vorlieben und Gefühle geben, werde schamlos Profit geschlagen. Unternehmen wie Google, Apple und Facebook sei nicht daran gelegen, dass wir uns im Internet wohler fühlen.

Ihr einziges Interesse gelte dem wirtschaftlichen Gewinn, der aus dem Datenüberschuss und Werbeverträgen errungen werde. Somit wird nicht nur eine liberaldemokratische Grundordnung der westlichen Wertegemeinschaft in Frage gestellt, sondern allen voran die informationelle Selbstbestimmung zutiefst beschnitten. Zuboff spricht hierbei von einem „Entziehungsakt durch Überwachung, der sich das Recht herausnimmt, jede Grenze in seinem Durst nach Kenntnis und Einfluss auf die detailliertesten Nuancen unseres Verhaltens zu ignorieren“ (15).

Demzufolge könnte der smarte Mensch nur als Randerscheinung einer neuen Kapitalismusform fungieren. Das Konstrukt des gläsernen Bürgers zu kritisieren würde bedeuten, lediglich an den Grundfesten einer Gesellschaftsordnung zu rütteln, die per se nicht an Persönlichkeitsrechten interessiert ist.

Das menschliche Verhalten wird zunehmend vorbestimmt, indem „Hilflosigkeit, Unachtsamkeit, Unannehmlichkeiten, Gewöhnung

oder Ablenkung“ (16) durch wirtschaftlich starke Konzerne gefördert und ausgenutzt wird. Die Folgen einer Entwicklung zum Überwachungskapitalismus sind im Detail unabsehbar. Daraus ergeben sich zahlreiche Negativszenarien, die Beachtung im Diskurs finden sollten (17).

Wesentlich trifft dies auf den Bereich der Privatheit zu, der nicht mehr aufrechterhalten werden könnte, wenn der Mensch unter permanenter technischer Überwachung steht. Dadurch würde nicht nur das Prinzip der Privatsphäre, sondern gleichfalls ein hohes Maß an Vertrautheit in der Gesellschaft verloren gehen. Hinzu kommt eine immense Machtasymmetrie, die durch die einseitige Erfassung, Verarbeitung und Kontrolle von Daten seitens der Geheimdienste und vieler Unternehmen entsteht. Spätestens seit den Veröffentlichungen Edward Snowdens ist klar, dass mitunter sogar Regierungen mit Konzernen wie AT&T zusammenarbeiten und Daten austauschen. Durch Praktiken dieser Art werden totalitäre Gesellschaftsentwicklungen gefördert, aber auch ein starkes Vertrauensverhältnis aufgrund wirtschaftlicher und sicherheitspolitischer Interessen leichtfertig aufs Spiel gesetzt (18).

Foucault'scher Erklärungsansatz

Kaum eine Alltagssituation ist letztlich frei von Überwachung: Seien es Überwachungskameras, Metadaten, die über Telefonate, SMS und Internetaktivitäten gesammelt werden, Kundenkarten, Navigationssysteme oder auch nur der Chef, der einem bei der Arbeit über die Schulter sieht. Das Gefühl des Beobachtetwerdens hat sich bereits in alltägliche Abläufe integriert und wird sogar in Form von Fitnessstrackern, bargeldlosem Bezahlen und Apps, die den Gemütszustand des Arbeitnehmers kontrollieren, bewusst angestrebt und gefördert (19).

Der Philosoph Michel Foucault beschreibt in *Überwachen und Strafen*, wie sich die Disziplinierung der Gesellschaft durch Institutionen und technische Hilfsmittel entwickelte. Er zeigt auf, dass Macht seit dem 17. und 18. Jahrhundert nicht mehr nur an eine Person gebunden ist, sondern zunehmend als eine Art Essenz existiere. Macht würde entindividualisiert, indem es durch Anordnung und Struktur der gesellschaftlichen Organe umgeformt werde. Das Verhältnis zwischen Machthaber und Machtlosen sei der Disziplinierung der Überwachung gewichen.

Besonders durch das Bentham'sche Konzept des **Panoptikums** (<https://denbegriffenaufdengrund.wordpress.com/tag/panoptikum/>) wird die Funktionsweise des Foucault'schen Souveränitätsmodells deutlich: Man muss sich das Panoptikum als großen, runden Raum mit einem Turm in der Mitte vorstellen. In den Wänden sind Gefängniszellen integriert; der Turm in der Raummitte fungiert als Wachturm, der mit starken Flutlichtern ausgestattet ist, die die Insassen blenden. So können die Gefangenen nie wissen, ob der Wachturm besetzt ist, und verhalten sich demnach immer diszipliniert. Somit reformiert sich die Dimension der Macht.

Die Macht ist durch den Turm allgegenwärtig sichtbar und dennoch nicht einsehbar. Dem Überwacher genügt eine sporadische Kontrolle, denn allein die Möglichkeit des Überwachtwerdens ist ausreichend, um Gefangene zu disziplinieren. Der Aufbau der panoptischen Institution bewirkt somit eine physisch gewaltlose Disziplinierung. Mittels detaillierter Daten und genauester Informationen, die ständig erhoben werden können, wird das Individuum subjektiviert und individualisiert. Parallel dazu erfolgt eine Objektivierung, da der Einzelne nur noch als Information gehandelt wird und nicht mehr Subjekt eigener zwischenmenschlicher Handlungen ist.

Foucaults historische Gegenwartsanalyse scheint sich im Zeitalter

des Internets offenbart, automatisiert und intensiviert zu haben. Das panoptische Gefängnis funktioniert massenhaft in vielen technologischen Formen. Persönliche Daten werden allerorts gesammelt.

Überwachungskameras und die Speicherung von Telekommunikationsdaten sind dabei nur ein geringfügiger Teil der Foucaultschen Disziplinartechnik. Mit der Erfindung des Internets wurde ein umfangreiches Medium geschaffen, in dem über Cookies, Tracker, Apps und Online-Käufe – um nur einige Instanzen zu nennen – eine sehr genaue Überwachung möglich ist: weltweit und in Echtzeit.

Viele der Neuerungen, die eine präzise Überwachung und Kontrolle ermöglichen, werden oft nur noch mit einem stillen Schulterzucken hingenommen. Dabei finden sich gegenwärtige Beispiele für Disziplinierungstaktiken nicht nur im Internet. So stieß die Einführung des neuen Polizeiaufgabengesetzes in Bayern und Sachsen auf erstaunlich wenig Widerstand, wenn man bedenkt, welche Willkür daraus hervorgehen kann (20). Warum rufen öffentlich präsenste Themen, wie die Anpassung des Polizeiaufgabengesetzes, Enthüllungen von Edward Snowden über die NSA oder von WikiLeaks über Möglichkeiten der Datenmanipulation durch die CIA, kaum noch Empörung hervor?

Ein beklemmendes Gefühl der Gegensätzlichkeit stellt sich beim Betrachten vieler Innovationen als Errungenschaft moderner freiheitsliebender Gesellschaftsmodelle ein. Einerseits nehmen die Wahlmöglichkeiten jeglicher Art zu, nicht nur aufgrund des hohen westlichen Lebensstandards, sondern vor allem auch durch die Vernetzung der Welt. Plötzlich ist der Zugang zu allem offen: Nachrichten, Unterhaltung, Wissen, aber eben auch zu vielen fraglichen Informationen, gezielt gestreutem Halb- oder Nichtwissen.

Andererseits sind nun auch die Negativfolgen einiger Innovationen zu entdecken: Automatisierte Überwachung, Kontrolle, Disziplinierung, Zensur. Diese stur auszublenken oder flüchtig zu belächeln, stellt keinen geeigneten Lösungsansatz dar. Vielmehr wäre es sinnvoll, einen öffentlichen Diskurs zu ermöglichen und zu fördern. Kommen staatliche Institutionen ihrer Pflicht nicht nach, liegt es im höchst eigenen Interesse der Bürger, zunehmende Disziplinierungsmaßnahmen zu hinterfragen: Kreditwürdigkeit nach Wohnadresse? Versicherungsprämien durch Fitness- oder Cartracking? Bargeldlose Zukunft? Unkontrollierte Sammlung und Verwendung personenbezogener Daten durch Sicherheitsbehörden und zukünftig durch ein neues Polizeigesetz?

Sinniert man über Foucaults Analyse in der Gegenwart, lauern die wachenden Augen längst nicht mehr nur in den Linsen regungsloser Überwachungskameras. Die Disziplinierungsmechanismen weiten sich um ein Vielfaches aus. Moderne Technik und Vernetzung ermöglichen den Verzicht auf direkt sichtbare Bauwerke wie ein Gefängnis im panoptischen Stil. Inzwischen kann Disziplinierung außerhalb einer Zelle und trotz vielfältigem Kontakt mit weiteren Individuen stattfinden.

Das „Mehr“ an Freiheit und Freiraum, das Bürger der westlichen Welt zu besitzen glauben, scheint auf ein „Weniger“ an Entscheidungsgewalt hinauszulaufen.

Ein Schulterzucken oder Abwinken ändert nichts an der Disziplinierungsdebatte, sondern fungiert im panoptischen Sinn geradezu als Rädchen, das die Maschine weiter antreibt (21).

Digitale Selbstverteidigung

Laut Ted Kaczynski folgen, wie eingangs erörtert, aus Innovationen unterschiedlichste gesellschaftliche Entwicklungen. Je mehr

Menschen durch eine Entdeckung in ihrem Alltag beeinflusst werden, desto größer erscheinen die verursachten Interdependenzen. Was als Einzelinnovation hilfreich wirkt, erscheint im Gesamtkontext plötzlich als Gefährdung. Somit gilt es, auch die Digitalisierung und das Internet zu hinterfragen, um eine offene und selbstständige Weltgesellschaft unter Wahrung der Persönlichkeitsrechte zu fördern. Otto Peters liefert mit seinem Buch *Kritiker der Digitalisierung* eine tiefgründige Sammlung an facettenreichen Standpunkten und eröffnet eine Vielzahl an Gesellschaftsfragen.

Allen voran der Standpunkt des Social-Network-Kritikers Jaron Lanier, der die Massenkultur des Internets insofern für fehlgeleitet hält, weil dadurch eine geistige Monokultur entstehe. Dies begünstige nicht nur die Manipulation, da Meinung über Denkschablonen kontrolliert werden könne, sondern schränke massiv die individuelle Denkfähigkeit ein. Hinzu kommt Laniers begründete Abneigung gegenüber dem Phänomen der Schwarmintelligenz. Dies stelle lediglich die „Durchschnittsmeinung einer anonymen Masse“ (22) dar und dürfe deshalb nicht als meinungsgebend in Onlinelexika wie Wikipedia durchgesetzt werden.

Allgemeiner formuliert der Softwareentwickler Bill Joy in seinem Essay *Warum die Zukunft uns nicht braucht*, dass Ethik und Wissenschaft entkoppelt seien. Ausgehend von dieser Erkenntnis fordert er die zunehmende Betrachtung ethischer Aspekte bei Innovationen und im Bereich der Forschung. Wissenschaft darf nicht losgelöst von moralischer Gesinnung gesehen werden (23). Dieser Kritikpunkt deckt sich mit einem Kommentar Harald Welzers in der TV-Sendung *Sternstunde Philosophie* des Schweizer Fernsehens. Dort führt er aus, dass durch Überwachung möglicherweise das Kriminalitätsproblem gelöst werden könne. Jedoch würde dies dann nicht aufgrund sittlicher Einsicht erfolgen, wie sie beispielhaft Immanuel Kant formulierte. Moralität könnte

sowohl durch Überwachung als auch durch Repression ersetzt werden.

Einen Hauptkritikpunkt an der Digitalisierung stellt demnach die Verlagerung und Verschleppung von Konfliktfeldern dar. Besonders im Bereich der suggerierten Sicherheit durch technische Maßnahmen bleibt offen, ob durch derartige Überwachung wahrhaft Kriminalität, Terrorismus und Skrupellosigkeit reduziert oder eben nur umgelagert oder gar angestaut werden. Nach der Zeit von Aufklärung, Freiheits- und Unabhängigkeitskriegen würde damit eine Phase der kontrollierten technischen Verlagerung von Konflikten beginnen.

Das kann in zweierlei Weise gedeutet werden. Einerseits führt diese Entwicklung zu moralischer Nachlässigkeit, da problemlösende Faktoren nicht mehr auf Sittlichkeit und ethischer Grundhaltung basieren. Andererseits werden überwachungskapitalistische Absichten begünstigt. Letzteres wäre eine Bestätigung der Thesen Shoshana Zuboffs in dem Sinne, dass Datenüberfluss nicht persönlichkeitsbildend, sondern einschränkend und totalitär wirkt.

Ein weiterer Standpunkt, der schwerwiegende Bedenken auslöst, betrifft soziobiologische Negativfolgen, die durch die regelmäßige Nutzung von technischen Endgeräten auftreten. Aric Sigman deutet damit an, dass der Verlust realer Interaktion zwischen Menschen von Angesicht zu Angesicht soziale Fehlentwicklungen bei Kindern, aber auch Fehlverhalten und Krankheiten bei Erwachsenen hervorrufen könne (24).

Eine Gesellschaft, die sich diesen biologischen Auswirkungen mithilfe eines unzulänglichen Gesundheitssystems anpasst, ist nicht an einer direkten Lösung orientiert.

Eben dadurch, dass, wie es beispielhaft der zunehmende Gebrauch

von Tablets in Schulen zeigt, den Negativfolgen nicht entgegengewirkt wird, entsteht eine weitreichende Akzeptanz für einen höchst schädlichen Lebensstil. Die Nachwirkungen beschränken sich im harmlosesten Fall auf Kurzsichtigkeit, Aufmerksamkeitsdefizite und Hyperaktivität. Doch das Fehlverhalten, das durch die Verarmung sinnlicher Interaktion entstehe, werde langfristige Veränderungen des menschlichen Gehirns begünstigen (25).

An dieser Stelle könnten weitere ernstzunehmende Risiken der stark digitalisierten Alltagswelt beschrieben werden. Die Liste der Nachteile scheint mindestens so lang wie die der Vorteile. Damit ergibt sich das Gesamtbild, welches gewiss vielen Innovationen innewohnt: ein Sammelsurium an Eigenschaften, die je nach Situation sowohl positiv als auch negativ zu bewerten sind.

Jedoch gibt es einen Faktor bei der Entwicklung des Internets, der smarten Welt und dem Internet der Dinge, der nicht erwähnt wird, weil keiner weiß, wie man ihn nennen soll. Er ist das gigantische Risiko, das eine komplett digitalisierte Gesellschaft mit sich bringt. Eine Welt oder ein System öffnet sich nicht nur, indem es sich per Kabel oder Frequenzen verbindet, sondern schränkt sich im selben Moment auch massiv ein, da die enorme Bündelung individueller Daten Machtinstrumente schafft, von denen keiner weiß, wozu sie verwendet werden können.

Beispielhaft dafür sind die Datenbanken von sozialen Netzwerken zu nennen, die eine gigantische Menge an persönlichen Informationen beinhalten. Totalitäre und menschenverachtende Regime – wie zu Zeiten der NSDAP in Deutschland – könnten mit dem Zugriff auf eben solche Datenbanken einen ungeheuerlichen Nutzen für ideologische Zwecke ziehen.

Das sind Arten von Gefahren, über die im Silicon Valley keiner spricht. Doch die Potenzialität besteht, und Innovationen lassen sich

nicht umkehren. Dieses und alle vorherigen Beispiele verdeutlichen, wie wertvoll informationelle Selbstbestimmung und wie wichtig somit digitaler Selbstschutz ist.

Bei Internetanwendungen auf Persönlichkeitsrechte zu verzichten oder dies mit einem Schulterzucken zu kommentieren, kommt der Selbstaufgabe und Selbstkommerzialisierung gleich. Die Achtung, die man im täglichen Leben vom Gegenüber einfordert, sollte man auch in einer digitalen Welt beanspruchen.

Umgang mit der Allgegenwärtigkeit des Internets

Diese Abhandlung kann leider nur einen winzigen Bruchteil einer unfassbar weitreichenden Thematik streifen. Die Essenz der Vielzahl an Berichten, Artikeln und Untersuchungen, die paradoxerweise häufig ausschließlich digital zur Verfügung stehen, erfasst ein überblicksartiges Gesamtbild: Eingangs wurde gezeigt, worin der konfliktreiche Faktor beim Sammeln und Verknüpfen von Daten besteht. Der Exkurs zu Michel Foucault hat einen besonderen Einblick in Mechanismen hinter Überwachungsstrukturen gegeben.

Erstaunlich ist hierbei, wie zeitgemäß sich sein Werk aus dem Jahre 1975 liest. Da wundert es nicht, dass man Foucaults Ausführungen nicht nur als Analyse, sondern auch als eine Art Anleitung verstehen kann. Im abschließenden Kapitel machte eine überblickshafte Zuspitzung die Gefahren deutlich, die von einer zunehmenden Digitalisierung ausgehen. Die Kernaussagen sind der vielfältige Charakter der Gesellschaftsrisiken und die Auswirkungen auf die menschliche Gesundheit.

Eben jene enorme Vielfältigkeit trägt als maßgebliches Charakteristikum zum Diskurs über digitale Anwendungen bei. Das

Spektrum an Einsatzmöglichkeiten stellt den Menschen vor eine ebenso große Fülle von Risikooptionen. Dabei bedeutet die Freiheit im Internet mehr als nur unbegrenztes Datenvolumen.

Informationelle Selbstbestimmung erstreckt sich über tiefgreifende Forderungen nach Persönlichkeitsrechten und korreliert mit Vorstellungen und Wünschen zu einer freiheitlich-demokratischen Grundordnung. Die Aufgabe der Autonomie im Internet würde leichtfertig totalitäre Herrschaftsformen begünstigen, deren Ausmaße aktuelle Dystopien weitaus übertreffen können.

Der gläserne Mensch stellt demnach kaum noch eine Metapher dar, sondern ist vielmehr bittere Wirklichkeit. Verantwortungslose, exzessive Internetnutzung und kommerzielle Unternehmensinteressen begünstigen diese Tendenz. Liegt zum einen die persönliche Datenvergabe in eigener Hand, sind zum anderen bestehende Datenschutzregelungen sehr unternehmensfreundlich, wenn es um das Abgreifen, die langfristige Speicherung und die Wiederverwertung von persönlichen Daten geht.

Letztlich ist die Einsicht notwendig, dass das Internet infolge der dadurch entstandenen weltweiten Vernetzung massive Gefahren in sich birgt. Besonders neuartige Innovationen im Internet der Dinge werfen prekäre Fragen rund um die Verwendung privater Daten auf.

Diesen Entwicklungen bedacht zu begegnen, sollte eine verantwortungsvolle Pflicht aller Gesellschaften darstellen.

Der ohnehin größtenteils westliche Diskurs zu Datenschutz und Datensicherheit sollte als Vorbild für künftige Kulturen gelten, die industriell-technologisch nachholen. Dazu gehört, die oben angesprochenen Risiken öffentlich zu hinterfragen und Lösungsansätze auszuarbeiten. Ein Schulterzucken darf nicht mehr akzeptiert werden. Bill Joys Aufforderung, Wissenschaft und Ethik

wieder zu vereinen, sollte nicht nur als Ratschlag, sondern als Grundvoraussetzung, sowohl für zukünftige Komiteebildungen als auch für Entscheidungen im Bereich Datenschutz und Datenspeicherung dienen.

Schließlich steht hinter all den Debatten, die sich um das Verhältnis zu Daten drehen, der Grundgedanke von Freiheit. Insofern darf Autonomie nicht als etwas Gegebenes, sondern sie muss als etwas Aufgegebenes verstanden werden. Denn grundsätzlich gelten Autonomie und informationelle Selbstbestimmung als Existenzbedingung des Menschen. Nur daraus lässt sich die nachhaltige Essenz menschlicher Freiheit bestimmen. Deshalb sollte jedem Menschen an der Wahrung und Umsetzung dieser Rechte gelegen sein – offline, und jetzt auch online.

Jan Schöpe, Jahrgang 1996, studiert Philosophie, Politikwissenschaften und Geschichte an der TU Dresden. Neben dem Studium arbeitet er am Lehrstuhl für Politische Theorie und Ideengeschichte. Dazu gehören nicht nur weitreichende Einblicke in den akademischen Alltag, sondern ebenso die Möglichkeit, Tutorien zu organisieren. Für seine Freizeit ist sportlicher Ausgleich und der Kampf gegen seine immer höher werdenden Bücherstapel essentiell.

Quellen und Anmerkungen:

(1)

<https://www.theatlantic.com/technology/archive/2010/10/goo>

[gles-ceo-the-laws-are-written-by-lobbyists/63908/](https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/)

[\(https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/\)](https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/)

(2) Vgl. BOGOST, Ian, 2015: Das Internet der Dinge, die wir nicht brauchen. In: Florian SPRENGER, Christoph ENGEMANN (Hrsg.): Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt. Bielefeld: transcript Verlag, S. 92f.

(3) Vgl. BUNZ, Mercedes, 2015: Die Dinge tragen keine Schuld: Technische Handlungsmacht und das Internet der Dinge, ebenda (2), S. 179

(4) **https://www.washingtonpost.com/lifestyle/style/how-publishing-a-35000-word-manifesto-led-to-the-unabomber/2015/09/18/e55229e0-5cac-11e5-9757-e49273f05f65_story.html**

[\(https://www.washingtonpost.com/lifestyle/style/how-publishing-a-35000-word-manifesto-led-to-the-unabomber/2015/09/18/e55229e0-5cac-11e5-9757-e49273f05f65_story.html\)](https://www.washingtonpost.com/lifestyle/style/how-publishing-a-35000-word-manifesto-led-to-the-unabomber/2015/09/18/e55229e0-5cac-11e5-9757-e49273f05f65_story.html)

(5) Vgl. KACZYNSKI, Theodor (1995): Industrial Society and Its Future. Lincoln, Absatz 125, 127, 128

(6) ebenda (5), Absatz 128

(7) WARREN, Samuel D., BRANDEIS, Louis D., 1890: The Right to Privacy. Harvard Law Review, 4 (5), S. 193–220, S.195

(8) **<https://www.menschenrechtskonvention.eu/konvention-zum-schutz-der-menschenrechte-und-grundfreiheiten-9236/>**
[\(https://www.menschenrechtskonvention.eu/konvention-zum-schutz-der-menschenrechte-und-grundfreiheiten-9236/\)](https://www.menschenrechtskonvention.eu/konvention-zum-schutz-der-menschenrechte-und-grundfreiheiten-9236/)

(9) KUHLEN, Rainer (2004): Informationsethik. Konstanz, S. 188

(10) Vgl. ebenda (9), S. 187f.

(11) Vgl. ebenda (9), S. 186f.

(12) Vgl. BOOTE, Werner (2015): Alles unter Kontrolle. (Film)

(13) Vgl. STRZOLKA, Rainer (2008): Das Internet als Weltbibliothek: Suchmaschinen und ihre Bedeutung für den Wissenserwerb. Berlin: Simon Verlag für Bibliothekswissen, S. 48f.

(14) Vgl. BULL, Hans Peter (2013): Netzpolitik: Freiheit und Rechtsschutz im Internet. (1. Aufl.). Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG.,

<https://doi.org/10.5771/9783845245881>

<https://doi.org/10.5771/9783845245881>), S. 65

(15) **<http://www.faz.net/1.4103616>** (**<http://www.faz.net/1.4103616>**)

(16) ebenda (15)

(17) Vgl. PETERS, Otto, 2012: Kritiker der Digitalisierung : Warner, Bedenkenträger, Angstmacher, Apokalyptiker; 20 Portraits /. Frankfurt am Main: Lang

(18) **<https://www.heise.de/tp/features/Die-brutalistische-Lauscharchitektur-von-NSA-und-AT-T-4092580.html>**

<https://www.heise.de/tp/features/Die-brutalistische-Lauscharchitektur-von-NSA-und-AT-T-4092580.html>

(19) **<https://mobilsicher.de/aktuelles/bigbrotheraward-negativpreis-fuer-arbeitnehmer-app-kelaa>**

<https://mobilsicher.de/aktuelles/bigbrotheraward-negativpreis-fuer-arbeitnehmer-app-kelaa>

(20) **<https://netzpolitik.org/2018/vorverlagerung-von-eingriffsbefugnissen-die-drohende-gefahr-in-polizeigesetzen/gl>**

<https://netzpolitik.org/2018/vorverlagerung-von-eingriffsbefugnissen-die-drohende-gefahr-in-polizeigesetzen/gl>

(21) Vgl. FOUCAULT, Michel (1997): Überwachen und Strafen. Frankfurt am Main, S. 279

(22) ebenda (17), S. 37

(23) **<https://www.wired.com/2000/04/joy-2/>**

<https://www.wired.com/2000/04/joy-2/>

(24) ebenda (17), S. 71f.

(25) ebenda (17), S. 92ff.

Dieser Artikel erschien bereits auf www.rubikon.news.



„Der Jugend gehört die Zukunft“ – und damit auch die Jugendredaktion Manovas. Um der angeblichen Politikverdrossenheit heutiger Jugendlicher entgegenzuwirken, zeigt Manova in der Kolumne „**Junge Federn** (<https://www.manova.news/kolumnen/junge-federn>)“, was die heranwachsende Generation beschäftigt, und zwar aus erster Hand. Denn hier haben junge Gastautoren und -autorinnen die Möglichkeit, unter der „Federführung“ von **Aaron Richter** als verantwortlichem Redakteur ihre persönliche Sichtweise auf aktuelle Themen zu präsentieren. Die Devise lautet: „Schreib uns, was dich bewegt; habe den Mut, die Stimme deiner Generation erschallen zu lassen. Denn es ist Zeit, dass diese Stimme gehört wird! “

Dieses Werk ist unter einer **Creative Commons-Lizenz (Namensnennung - Nicht kommerziell - Keine Bearbeitungen 4.0 International** (<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>)) lizenziert. Unter Einhaltung der Lizenzbedingungen dürfen Sie es verbreiten und vervielfältigen.