Heinz Kleger/Eric Makswitat

Der Snowden-Effekt

Warum eine Zivilgesellschaft digitalen Ungehorsam braucht

Josef K., der Protagonist aus Franz Kafkas *Der Prozess,* erwacht eines Morgens und wird »ohne daß er etwas Böses getan hätte« verhaftet. Niemand will dergleichen erleben und doch überrascht der bisher nur sehr unzureichende Protest der inzwischen protesterfahrenen Deutschen gegen die massenhafte Überwachung durch fremde und eigene Geheimdienste. Dies liegt möglicherweise in der Tatsache begründet, dass nur wenige wirklich glauben, sie besäßen wichtige Informationen, die abschöpfungswürdig wären. Dabei gilt doch, dass es keine unsensiblen Daten mehr gibt. Nicht nur staatliche Stellen bedienen sich, auch Unternehmen wie Google, Amazon und Microsoft zeigen großes Interesse an der Verfügbarkeit von Meta-Daten. Denn viel wichtiger als der spezifische Inhalt der Kommunikation ist heute die Struktur und das Muster der Daten. Es ist interessanter zu erfahren, welcher User wie auf eine Seite im Internet gelangt ist, als das Wissen darüber, was die Webseite zeigt.

Edward Snowden ist zweifellos ein Super-Whistleblower. Seine Enthüllungen im letzten Jahr stellen in mehrfacher Hinsicht einen Wendepunkt dar. Es wird offenbar, dass die Überwachung durch die Geheimdienste sich nicht nur gegen den internationalen Terrorismus richtet, wie immer behauptet wird. Die Geheimdienste verletzten systematisch ihre Rechenschaftspflichten gegenüber den Regierungen. Anders ist die Überwachung des Mobiltelefons der Kanzlerin wohl kaum zu bewerten. Ausgestattet mit Beschlüssen des geheim tagenden FISA-Gerichts (Foreign Intelligence Surveillance Act, Gesetz zum Abhören in der Auslandsaufklärung) zwingt beispielsweise der amerikanische Geheimdienst NSA Technologiefirmen zu stetigen Zugriffsmöglichkeiten. Das massenhafte Abgreifen der Daten direkt vom unternehmenseigenen Server wird somit möglich. Der positive Nebeneffekt dabei ist: Digitale Aktivisten können nun nicht länger als paranoid abgestempelt werden, sie warnten seit längerem vor Totalerfassung und -überwachung.

Die Überwachung der eigenen Daten ist erstmals in der Geschichte global geworden. Der Enthüllungsjournalist Glenn Greenwald sprach in diesem Zusammenhang von der unterschiedslosen Massenüberwachung. Allein das Wissen um die mögliche Überwachung verändert das eigene Kommunikationsverhalten. Wer sich überwacht fühlt, der verändert die eigene Kommunikation oder schränkt sie ein, was ein geradezu unglaublicher Vorgang in einer liberalen Demokratie ist. Wer gibt schon die eigene Selbstzensur zu? Wem kann man in dieser Situation noch vertrauen, wie kann man sich dagegen wehren? Diese Fragen werden vor allem in der sogenannten Netzgemeinde verstärkt diskutiert. Bisher wurde die Datensouveränität im Begriff der Bürgersouveränität nicht berücksichtigt.

Nun wird offensichtlich, dass die Geheimdienste nicht länger kostspielige und langwierige Observationen vornehmen müssen, um an die gewünschten Informationen zu gelangen: Die Auskünfte stehen schließlich bereits im Netz, die Nutzer haben sie selbst dort hochgeladen. Digitale Bewegungen, die ihre Daten schützen oder verteidigen, werden also immer wichtiger. Auch für die Netzutopisten geht es nicht mehr um die grenzenlose, sondern um die konkrete alltägliche Freiheit, die ständig Machtkonflikte riskieren muss.

Netzpolitiker, Hacker und Aktivisten fühlen sich bedroht. Whistleblowing ist nur ein Teil ihres digitalen Ungehorsams. Weitere Methoden werden in unserem Aufsatz »Digitaler Ungehorsam. Wie das Netz den Zivilen Ungehorsam verändert.« (Forschungsjournal für Neue Soziale Bewegungen 4/2014) aufgeführt. Das Netz hat den zivilen Ungehorsam verändert, die Situation des Widerstandes ist neu. Digitale Aktivisten sind beileibe keine Verfassungs- oder Staatsfeinde. Gerade Snowden berief sich stets und ausdrücklich auf den vierten Zusatzartikel in der amerikanischen Verfassung. Sein ziviler Ungehorsam ist verfassungspatriotisch motiviert im amerikanischen Sinne: Vaterlandsliebe und der Wunsch, die amerikanische Verfassung zu verteidigen, führten ihn genauso zur National Security Agency, dem überfinanzierten und mit 40.000 Mitarbeitern größten Geheimdienst der westlichen Welt, wie zum digitalen Ungehorsam. Sein Fall ist deshalb politisch zu diskutieren, er hat eine politische Intention.

Insgesamt sind Aktivisten des digitalen Ungehorsams auch keine Denunzianten oder Spione, was naheliegen könnte, denn mit ihrem Wissen wäre viel Geld bei anderen Geheimdiensten zu verdienen. Sie entscheiden sich stattdessen für eine mutige Veröffentlichung, welche die liberale Öffentlichkeit, die selber in einer Krise der Kommerzialisierung, Boulevardisierung und Personalisierung steckt, informieren und aufwecken soll. Es ist der klassische moralisch-politische Appell des zivilen Ungehorsams in einer diesbezüglich weitgehend passiven Mehrheitsgesellschaft. Dieser zivile Widerstand oder bürgerliche Ungehorsam beansprucht »öffentlich« und »friedlich« sowie »moralisch-politisch« begründbar zu sein: Je besser er begründet ist, desto legitimer ist er. Trotzdem spielt er Legitimität nicht gegen Legalität aus. Obwohl eine »tatbestandliche Rechtsverletzung« vorliegt, kämpft er politisch um das Recht und innerhalb des demokratischen Rechtsstaates, auf dessen Funktionieren er bauen und vertrauen muss. Oft ist Rechtswandel durch diese Art von zivilem Rechtsbruch erst eingeleitet worden. Der Legalismus ist dabei ebenso umstritten wie die Legitimitätspolitik.

Es ist paradox, mit welcher Härte liberale Demokratien Whistleblower und digitale Aktivisten verfolgen und bestrafen, obwohl sie Wichtiges gerade für den Rechtswandel leisten. Ebenso werden Journalisten und ihre Angehörigen behindert, die sich dieser Aktivisten annehmen. Der Lebensgefährte von Glenn Greenwald, David Miranda, wurde beispielsweise mehrere Stunden wie ein Schwerverbrecher am Londoner Flughafen Heathrow festgehalten, untersucht und befragt, nur weil vermutet wurde, er hätte Daten von Edward Snowden bei sich. Zur Anwendung kam dabei ein Anti-Terror-Gesetz – ein Gesetz, das eingeführt wurde, um Terroristen wie Osama Bin Laden zu stoppen.

Bisher hing das Ansehen westlicher rechtsstaatlicher Demokratien auch davon ab, wie sie mit ihren Gegnern, ja selbst mit ihren Feinden, die es gibt, umgehen. Dass sie dabei an rechtsstaatlichen Garantien festhielten, hat sie nicht geschwächt. Die attraktive Integrationskraft einer entschiedenen Toleranz der Demokratie hat sie vielmehr gestärkt. Die Fähigkeit zur Selbstkritik und Selbstkorrektur konnten sich die westlichen Demokratien bei all ihren Defiziten immer zugutehalten. Eine liberale Anarchie der Werte folgt daraus ebenso wenig wie eine Diktatur des Relativismus. Die Toleranz der liberalen Demokratie, die vieles integrieren und zugleich verändern kann, ist zwar weich (Lenin würde abwertend sagen »demokratieweich«), aber sie ist nicht schwach. Das ist zweierlei.

Entschiedenheit und Toleranz

Heute existiert eine antitotalitäre Entschiedenheit im Grundsätzlichen aufgrund leidvoller historischer Erfahrungen. Diese bilden einen Legitimationsanker, sowie

ein Eingeständnis eigener Schwächen, das den Weg zur Selbstkritik offen hält. Beides kompensiert das Einheitsdefizit einer liberalen Demokratie, die primär ergebnisoffen und verfahrensorientiert ist. Der demokratische Verfassungsstaat ist sowohl ein Experiment der Freiheit als auch ein Experiment der Wahrheit. Will man starke Bürgerinnen und Bürger, so stärkt man ihre zivilen Tugenden durch Wissen und Fähigkeiten. Auf die Frage, warum er sich entschieden habe, zum Whistleblower zu werden, antwortete Snowden, »dass er innerhalb des Systems gekämpft habe, bevor er zum Schluss gekommen sei, dass es keine andere Alternative gebe, als sich an die Außenwelt zu wenden« und die Innenwelt sich verselbstständigender und unkontrollierter Staatsapparate zu verlassen. Wenn Bürgersouveränität in einer modernen Welt auch Datensouveränität heißt, so hat er dieser einen Dienst erwiesen.

Die Technologien sind schneller gewachsen als die Gesetze. Geheimdienste haben sich diesen Umstand zunutze gemacht und umfangreiche Abhörmechanismen entwickelt, zum Beispiel Unterseekabel durch Drohnen anzubohren, um so Internetverbindungen anzuzapfen. Diese vielfältigen Aktivitäten sind offenbar weder strafbar noch explizit erlaubt. Als Ausrede wird geltend gemacht, man bewege sich ja im Rahmen der Gesetze. Alles, was möglich scheint, wird erfinderisch und ohne Rücksicht gemacht, insbesondere dann, wenn man meint, dadurch die eigenen positiven Werte zu verteidigen und sich im Krieg gegen den Rest der Welt zu befinden. Die »höhere Amoralität der Politik« (Luhmann), die Freiheit im Überwachungsmodus zu verteidigen, kommt hier super-machiavellistisch zum Zug. Dies ist gerade in Zeiten der Fall, wo allerorten die Machtpolitik mit Macht wieder zurückkehrt. Ein Imperium lässt sich nicht mäßigen, auch unter Freunden nicht. Das gescheiterte No-Spy-Abkommen zwischen Deutschland und den USA belegt dies. Der angebotene Cyberdialog ist nicht viel mehr als ein Zückerchen.

Die Enthüllungen von Edward Snowden haben gezeigt, dass die eigenen Landsleute ebenso ins Visier der Geheimagenten geraten können wie Bürger aus anderen Staaten. Besonders das britische Government Communications Headquarters (GCHQ) arbeitet eng mit der NSA zusammen: Viele europäische Verbindungsdaten passieren Großbritannien, bevor sie in die USA gelangen. Vielfach agiert die britische Regierungsbehörde umfangreicher als es die Amerikaner je könnten. Der Titel eines Überwachungsprogramms von GCHQ lautet bezeichnenderweise »Die Beherrschung des Internets« *(Mastering the Internet)*.

Wie reagiert darauf die liberale Öffentlichkeit, zum Beispiel in der Bundesrepublik? National gedachte Lösungen, wie sie die deutschen Telefonprovider mit ihrer Aktion »E-MAIL MADE IN GERMANY« forcieren, sind Marketingaktionen und dienen nicht der Herstellung von umfangreicher Datensouveränität. Digitale Aktivisten wählen einen anderen Weg, indem sie sich durch Verschlüsselung entweder abschotten oder Abwehrmaßnahmen forcieren. Sie befinden sich dabei nicht im Kriegszustand, sie haben nur das eine Ziel, durch ihren digitalen Ungehorsam Debatten in der Öffentlichkeit zu entfachen, die politische Wirkungen haben sollen. Dieter Deiseroth verlangt deshalb in seinem Artikel »Whistleblowing und ziviler Ungehorsam im demokratischen Verfassungsstaat« (NG/FH 1+2/2014) die Einführung von umfangreichen Whistleblower-Schutzgesetzen auch in der Bundesrepublik Deutschland: »Die Rechtslage bei uns in Deutschland schützt Whistleblower leider nur sehr unzureichend.« »Schwere Rechtsbrüche (...) verdienen keinen Schutz.« Dazu gehört auch der Verfassungsbruch durch den Bundesnachrichtendienst (BND), indem er vielfach das Grundrecht auf Privatsphäre verletzte. Der

BND und die NSA arbeiten seit Jahrzehnten zusammen, wenn auch nicht auf Augenhöhe, wie die mutmaßlichen CIA-Doppelagenten zeigen.

Deiseroth hat recht, allerdings vergisst er die anderen Formen des digitalen Ungehorsams. So fehlt der Hinweis auf »Anonymous« und »Wikileaks«, ebenso werden die Hackerkultur und die Netzwerke oder die digitale Diaspora in Berlin nicht erwähnt. Der US-Amerikaner Jacob Appelbaum, IT-Forscher und Hacker, lebt seit einiger Zeit in Berlin und sieht den Widerstand im Netz erst am Anfang. Die Hackerszene in Deutschland ist dank des Chaos Computer Clubs historisch stark, und Aktivisten fühlen sich angestachelt von den Enthüllungen Snowdens. Initiativen wie »Reset the Net« (resetthenet.org) stellen Sammelbecken für die konzentrierte Unzufriedenheit der netzbasierten Protestbewegung dar. Diese Phänomene sind Beispiele, die für eine ausführliche und genaue Diskussion genutzt werden sollten. Hinzu kommen Künstlervereinigungen wie die »!Mediengruppe Bitnik« aus Zürich oder das »Peng!Collective«, die Medienhacks betreiben, um die schwache Zivilgesellschaft auf das Thema Überwachung hinzuweisen. Internetaktivisten treten außerdem als außerinstitutionelle Veto-Spieler auf, die durch »Leaks« und digitale Protestformen ganze Gesetze verhindern können, wie das 2012 im Fall ACTA geschehen ist. Die Verhandlungen um das Freihandelsabkommen TTIP sind davon ebenfalls betroffen.

Weit offensiver gehen Aktivisten vor, die sich der Denial-of-Service-Attacke (DDoS) bedienen. Sie überlasten Server, auf denen Webseiten von Unternehmen oder Regierungsstellen lagern, mit einer Vielzahl an Anfragen. Die Webseiten sind dann für eine gewisse Zeit nicht erreichbar. Schon heute gilt, dass wer nicht erreichbar oder online ist, womöglich gar nicht existiert. Solche Attacken zielen auf die Meinungsfreiheit und sind daher kritisch zu bewerten. Deiseroth vernachlässigt in seinem Artikel überdies die Motivlage der Whistleblower und digitalen Aktivisten, zum Beispiel deren Frustration darüber, dass eine Mehrheit noch immer Parteien wählt, die der (faktisch unbegrenzten) Überwachung nicht Einhalt gebieten.

Das Internet mit seinen Möglichkeiten der sozialen Vernetzung, des Konsums, der politischen Aktion, der Entfaltung und Zerstreuung ist inzwischen Teil einer Auseinandersetzung zwischen Generationen. Bei beiden Gruppen – der »analogen« und der »digitalen Generation« – manifestiert sich seit den 80er Jahren das Bewusstsein der zwei Welten, der realen und der virtuellen. In der realen Welt gibt es feste Regeln, Normen und Eliten, die den Zugang zum Wissen streng kontrollieren; im Netz hingegen beschränken lediglich die technischen Grenzen das neue Kommunikationsmedium. Je leistungsfähiger die Computer, umso schneller der Internetzugang und je größer die elektronische Nutzerschaft, desto größer wurde das Unverständnis in der Debatte zwischen Netzoptimisten (»digitale Generation«) und Netzkritikern (»analoge Generation«). Über die Jahre hinweg bildeten sich so konträre politische Ansichten heraus. Die Aktivisten wenden sich dabei nicht gegen eine Verrechtlichung des Netzes, denn neue Rechte schaffen zweifellos auch neue Freiheiten. Problematischer wird dagegen der Versuch bewertet, nationales Recht auf das Internet und seine Kommunikationswege anzuwenden. Aus ihrer Sicht darf es kein amerikanisches, chinesisches oder ein deutsches Internet geben, sondern nur *ein* Internet, in dem allein internationales Recht wirkt. Alles andere verkennt die Struktur und die Funktionsweise des Netzes als globales Medium.

Ebenso wichtig ist an dieser Stelle die kritische Diskussion des sogenannten »Supergrundrechts« auf Sicherheit, von dem der ehemalige Innenminister Friedrich sprach. Hier ist Sicherheit nicht nur eine Bedingung der Freiheit wie in der klassi-

schen Tradition der politischen Theorie des Verfassungsstaates von Montesquieu, der davon spricht, dass »gemäßigte Regierungen« so eingerichtet werden müssen, dass »Bürger einander nicht zu fürchten brauchen«. Das vorherrschende Sicherheitsdenken geht heute nicht nur der Freiheit voran, sondern wird ihr selbst gegenüber den Grundrechten übergeordnet. Der Fall Snowden ist ein Beispiel dafür. Schließlich bleibt von der selbstbestimmten Freiheit nicht mehr viel übrig, weil man zu eingeschüchtert ist, um überhaupt noch frei sein zu können. Das fehlende Handeln-Können ist ein Indiz dafür: Zu vieles wird hingenommen bis hin zur »freiwilligen« Aufgabe der Privatheit in der Spaßgesellschaft, so dass man von einer Naivität und Unverbindlichkeit sprechen kann, vor der man sich wiederum fürchten muss.

Wie lässt sich in dieser Situation der zivile Widerstand von Bürgern verstehen? Die digitalen Aktivisten ringen derzeit um neue Narrative, um überzeugen und mobilisieren zu können. Sie sehen ihren Netzutopismus in Gefahr und versuchen die NSA-Systeme durch Verschlüsselungssysteme zu bekämpfen. Das jeweilige Bedrohungsszenario bestimmt die Maßnahme, digitale Selbstverteidigung heißt der erste Schritt.

Während Deiseroth den neuen zivilen Ungehorsam ernstnimmt, argumentiert Kurt Graulich in seinem Artikel »Blowing in the wind? NSA, Snowden und die Rechtslage für Whistleblower in Deutschland« (NG/FH 4/2014) mit alten Argumenten gegen ihn. Er verteidigt die Kultur des Staatsgeheimnisses und sieht in den Enthüllungen von Snowden keine Debattenrelevanz für Deutschland. Dies obwohl der BND zum Beispiel mit der NSA regelmäßig Informationen ausgetauscht hat, darunter auch Metadaten. Außerdem gab er die eigenen digitalen Spionagesysteme, Mira 44 und Veras, weiter. Ein Snowden-Dokument belegt sogar, dass die NSA am 7. Januar 2013 allein in Deutschland 16.000.000 Kommunikationsverbindungen überwacht hat. Das Parlamentarische Kontrollgremium ist seiner Funktion wohl kaum gerecht geworden. Damit steht nicht weniger als der gewaltenteilige demokratische Verfassungsstaat auf dem Spiel, wenn der »Leviathan« als Sicherheits- und Überwachungsstaat, der »Schrecken« erzeugen soll (Hobbes), nicht mehr gezähmt werden kann. Das Parlament sollte die Geheimdienste kontrollieren und nicht umgekehrt.

Digitaler Ungehorsam als ziviler Ungehorsam

Graulich sieht indes keine Notwendigkeit, zum zivilen Ungehorsam zu ermuntern, obwohl Henry David Thoreau, der Mahatma Gandhi und Martin Luther King inspirierte, bereits sagte: »Die rechtmäßige Regierungsgewalt, selbst wenn ich bereit bin, mich ihr zu unterwerfen, (...) ist immer unvollständig: Um nämlich unbedingt gerecht zu sein, muss sie Vollmacht und Zustimmung der Regierten haben«. Statt auf Argumente in der Tradition des zivilen Ungehorsams einzugehen, der weder das Recht in die eigene Regie nimmt noch das Gewaltmonopol des Staates in Frage stellt, wird stattdessen (einmal mehr) Carl Schmitt ins Feld geführt, welcher 1932 wirkungsvoll Legitimität gegen Legalität ausspielte. Schmitt hatte sich für die »demokratische Substanz« der Verfassung (Legitimität), deren Hüter der Reichspräsident sein sollte, und gegen den Rechtspositivismus mit seinem »Mehrheitsfunktionalismus« (Legalität) positioniert. Solche ideengeschichtliche Überblendungen, die manchmal lehrreich sein können, führen jedoch nicht immer zu einer angemessenen Dramatisierung der gegenwärtigen Lage. Politische Theorie, die in Geschichte nicht aufgeht, ist vor allem eine Schule der Urteilskraft, für welche die konkrete Wahrnehmung entscheidend ist. Die Augen-Metaphorik bei Aristoteles ist kein Zufall; es ist zu »sehen«, dass die Handlung angemessen oder unangemessen ist.

In Entgegnung auf Graulich und Schmitt könnte man sagen: Souverän ist heute, wer über die Kontrolle seiner Daten verfügt. Zur Bürgersouveränität als Baustein der Volkssouveränität gehört die Datensouveränität. In der deutschen Philosophie fehlt die Tradition eines selbstverständlichen (kleinen) Widerstandsrechts von sich demokratisch verstehenden Bürgerinnen und Bürgern. »Die Wahrheit auszusprechen, ist zudem kein Verbrechen«, so Snowden, der sich mutig und allein gegen eine »allmächtige, automatisierte Massenüberwachung« wandte. Solche Überwachung führt zu Konformität, aber auch zu Angst und Misstrauen. Dadurch wird ebenso das vertikale Vertrauen (zu Regierung und Staat) wie horizontales Vertrauen (zwischen den Bürgern) zerstört.

Wir leben in einem Zeitalter von Big Data, in dem Geheimdienste vom Besonderen zum Allgemeinen übergehen. Nicht länger geraten nur gefährliche Personen oder Gruppen ins Visier, sondern das gesamte Kommunikationsverhalten wird an verschiedenen Stellen auf Vorrat gespeichert. Was die rechtsstaatliche Strafverfolgung und das Schicksal eines Individuums angeht, so sind der deutschen Regierung zurzeit die strategischen Beziehungen zu den USA offenbar wichtiger. Snowden erhielt in Deutschland kein Asyl. In den USA erwartet ihn kein faires Verfahren. Von freundlichen »civilizern« ist wenig geblieben. Diese Furcht der Regierung, die im Unterschied zu den Ängsten der Bürger gänzlich unbegründet ist, ergänzt die Furcht der Individuen vor der Freiheit.

Digitaler Ungehorsam versucht Unrecht gegenüber anderen abzuwenden und nicht gleichgültig die bewusste oder unbewusste Grenzübertretung zum eigenen Vorteil zu legitimieren. Er steht für neue Protestformen im Netz. Das Ziel ist die Schaffung von Öffentlichkeit und die Auslösung von Debatten. Viele Aktionen sind kreativ, da sie geradezu spielerisch mit der Überwachungsthematik umgehen, andere blockieren und einige zerstören sogar Kommunikation, was natürlich auch problematische Aspekte hat.

Der Protest zielt jedoch auf eine Zivilgesellschaft, die zu leichtfertig mit ihren rechtsstaatlich garantierten Freiheiten umgeht. Bürgerrechte sind grenzüberschreitend ernst zu nehmen. Snowden stellt eine praktische Lösung in der Debatte um den neuen Ungehorsam dar. Zuvor wurde der digitale Ungehorsam als Störung verstanden. Mit Snowden erhält der Widerstand im Netz eine neue Bedeutung und Dimension. Die Zivilgesellschaft ist deshalb gefragt, die von Snowden angestoßene Diskussion weiter am Leben zu erhalten. Deutschland hat Handlungsbedarf beim Whistleblowerschutz, gleichzeitig muss die Empörung aufgegriffen, der Ungehorsam verstanden und in Handeln umgesetzt werden. Weniger angebracht ist ein politischer Werteopportunismus, der den Schutz von Grundrechten, wozu das Recht auf Privatsphäre gehört, ignoriert und faktisch zur Disposition stellt. Der digitale Ungehorsam hat auf diesen Umstand aufmerksam gemacht.

Heinz Kleger
ist Professor für Politische Theorie an der Universität Potsdam.

kleger@uni-potsdam.de

Eric Makswitat
ist FES-Stipendiat und studiert Politikwissenschaft an der Universität Potsdam.

eric.makswitat@uni-potsdam.de