Digitaler Ungehorsam

Wie das Netz den zivilen Ungehorsam verändert

Heinz Kleger/Eric Makswitat

Der ehemalige Bundesinnenminister Hans-Peter Friedrich erklärte im Zuge der Debatte um die Enthüllungen des US-amerikanischen Whistleblowers Edward Snowden, dass die Sicherheit Vorrang vor jedem anderen Grundrecht hat und damit ein „Supergrundrecht" sei. Die Aufdeckung der Abhörpraxis verschiedenster Geheimdienste durch Snowden wird ihm daher als grobe Störung, wenn nicht gar als Gefahr vorgekommen sein. Während Hans-Peter Friedrich Snowden als Störquelle für die Sicherheit der Bundesbürger identifiziert, hat jüngst der amtierende Bundesinnenminister Thomas de Maizière Snowden als „Rechtsbrecher" bezeichnet. Im Gegensatz dazu übersetzt der Wissenschaftliche Dienst des Deutschen Bundestages den englischen Begriff „Whistleblower" mit „Hinweisgeber mit Zivilcourage" und ermöglicht damit eine positive Deutung (Bug/Beier 2009).

Vor dem Hintergrund dieser ambivalenten Bewertung der Person des Whistleblowers stellt sich der Beitrag die Frage nach dem demokratischen Potenzial von digitalen Protestformen und -akteuren. Dazu gehört beispielsweise das „Whistleblowing", aber auch Distributed-Denial-of-Service-Attacken (DDoS - eine Vielzahl an Anfragen sinnloser Zeichenketten, die dafür sorgen, dass der Server, auf der eine zu blockierende Webseite lagert, zusammenbricht), wie sie häufig von der Anonymous-Bewegung ausgeführt werden. Hinzu kommen öffentlichkeitswirksame Auftritte und Protestaktionen von Internetaktivisten wie Julian Assange, Jacop Appelbaum oder der „!Mediengruppe Bitnik" aus Zürich. Kann dieser digitale Ungehorsam als eine neue Form zivilen Ungehorsams verstanden werden? Die Analyse und der Vergleich dieser Beispiele sollen aufklären, ob es sich hierbei um eine Art des digitalen Ungehorsams handelt, der als neue Form zivilen Ungehorsams verstanden werden kann.

Ausgangspunkt ist das normative Verständnis eines gerechtfertigten zivilen Ungehorsams als eine Möglichkeit des Widerstandes. Der digitale Ungehorsam wäre dann eine auf das Internet fokussierte Variante, die in den liberalen Demokratien eine gerechtfertigte Widerstandsform demokratischen Protestes wäre. In dieser Hinsicht würde das Handeln von Snowden legitim sein und könnte auch nicht durch den Hinweis auf die Sicherheit kriminalisiert werden. Es mutet grotesk an, dass die in den letzten Jahren bekannt gewordenen Protestakteure des Internets entweder zu langen Haftstrafen verurteilt oder mit Auslieferungsverfahren versehen wurden. Gleichzeitig flüchten sie in Länder wie Russland, China oder Ecuador, die allesamt keine liberalen Demokratien sind. Offenbar deswegen, weil die westlichen Demokratien ihre Enthüllungen als großes Sicherheitsrisiko und nicht als notwendige demokratische Maßnahmen zur Schaffung von Öffentlichkeit wahrnehmen.

1 | Neue Protesthandlungen

Die Funktionsweise des Internets verändert Entstehung, Wirkungsweise und Folgen von Protesthandlungen. So greift die Definition des zivilen Ungehorsams nicht mehr vollständig, wenn von im Netz geborenen Protestaktionen gesprochen werden soll, die für sich politische Partizipation in Anspruch nehmen. Eine ausführliche begriffliche Veränderung und Beschreibung, welche die neue Dynamik, die Kriterien

sowie die noch nicht ausdiskutierten Legitimitätsfragen der elektronischen Protestkonzepte berücksichtigt, steht aus, und das, obwohl sich seit den 1990er Jahren zahlreiche Wortkombinationen und -neuschöpfungen finden, die den Begriff des zivilen Ungehorsams auf den netzbasierten Protest auszuweiten versuchen.

Der Ausdruck „electronic civil disobedience" wurde von amerikanischen kapitalismus- und medienkritischen Künstlern geprägt, die sich im Künstler-Kollektiv „Critical Art Ensemble" organisieren. In ihrem Buch von 1996 mit dem Titel „Electronic civil disobedience and other unpopular ideas" finden sich die ersten ausführlichen Auseinandersetzungen mit der Thematik (Critical Art Ensemble 1998). Darin wird von der Notwendigkeit gesprochen, den zivilen Ungehorsam neu zu denken. Schlachtrufe wie „Auf die Straße!" funktionieren demnach bei aktuellen Themen nicht mehr. Die Autoren konstatieren, dass der zivile Ungehorsam vielleicht auf lokaler Ebene noch zu Ergebnissen führt, aber seine Durchsetzungskraft insgesamt schwindet. Neue Modelle der Störung werden folglich unter dem Begriffspaar des „electronic civil disobedience" gefasst. Es wird konstatiert, dass die gezielte Unterbrechung der elektronischen Informationsbewegung Institutionen stärker lähmt und langfristig sogar ihren Kollaps bedeuten kann. Die immer größer werdende globale Vernetzung von Organisationen, Unternehmen und staatlichen Institutionen lässt die Anfälligkeit für diese neue Form des Ungehorsams zunehmen. Für diese Autoren sind folglich die Jugendlichen ihrer Zeit die neuen Revolutionäre, die für den freien Zugang zu allen Informationen „kämpfen". Ganz im Sinne einer Transparenzgesellschaft, in der das Wissen frei zugänglich ist und die Verknüpfung von Macht und Information sich löst.

Die jugendlichen Einzelkämpfer von damals sind nun selbst zu politischen Aktivisten mit einer Agenda und zahlreichen Mitstreitern geworden, geboren aus der Hacker-Kultur der 1980er- und 1990er-Jahre. Wenn Hacker ihre Fähigkeiten ausschließlich als Protestmittel wahrnehmen, dann wird vom „Hacktivismus" (engl. Hacktivism) gesprochen. John Perry Barlow skizzierte 1996 in seiner „Declaration of Independence for Cyberspace" die Grundidee des Hacktivismus (Barlow 1996). Dazu zählen Protestmittel wie die unberechtigte Veränderung einer Webseite (Defacement), eine Distributed-Denial-of-Service Attacke (DDoS), Ping Storms (funktionieren ähnlich wie DDoS-Attacken), Email Bombing (Spam), Malicious Code Attacks (Einschleusen von Viren und Würmern), Redirects (die Weiterleitung fremder Webseiten auf eigene Server) und anderes mehr. Dieser „Hacktivismus" ist jedoch nur ein Teil des von uns zu definierenden digitalen Ungehorsams.

Um sich dem Begriffspaar digitaler Ungehorsam anzunähern, müssen vorab drei Formen des Ungehorsams genauer betrachtet werden. Es handelt sich hierbei um Beispiele, die ihren Ursprung im Internet haben oder von der breiten Öffentlichkeit des Netzes maßgeblich profitieren. Zuerst folgt die Auseinandersetzung mit dem bereits angeführten Whistleblower, einem Hinweisgeber, den es nicht erst seit der Erfindung des Internets gibt, welchem aber die neuen Möglichkeiten anonymer Veröffentlichung im World Wide Web gelegen kommen. Danach folgt die Beantwortung der Frage: Wer oder was ist „Anonymous"? Anschließend wird exemplarisch Julian Assange als berühmter Internet-Aktivist herangezogen, um schließlich den Weg zu einer Erklärung digitalen Ungehorsams zu ebnen.

2 | Whistleblower

Die wörtliche Übersetzung des englischen Begriffs ist „Pfeifenbläser" im Sinne von jemandem „in die Pfeife blasen" oder „jemanden verpfeifen". Früher wurde darunter ein Alarmpfiff eines Polizisten verstanden, der die Öffentlichkeit auf etwas aufmerksam machen wollte. Heute steht der Ausdruck für eine Person, die auf geheime Missstände hinweist (Groneberg 2011: 34). Ein deutsches Wort für den Whistleblower zu finden, gestaltet sich als

schwierig, denn Übersetzungen wie „Denunziant„, „Verräter“ oder „Querulant“ haftet ein negativer Beiklang an; sie werden der englischen Bedeutung des Wortes nicht gerecht. Eine Rückkehr des Denunzianten, der für Diktaturen eine unverzichtbare Rolle spielt, wünscht sich niemand.

„Whistelblowing“ wiederum wird unterschieden in internes und externes „Whistleblowing“. Internes „Whistleblowing“ geschieht gegenüber dem Arbeitgeber; das heißt, eine dort im Betrieb beschäftige Person wendet sich aufgrund einer Unrechtmäßigkeit an den Betriebsrat, den Abteilungsleiter oder an einen Ombudsman. Geht der zukünftige Whistleblower jedoch direkt zu einer zuständigen Behörde (beispielsweise zum Gesundheitsamt), zur Polizei oder zu den Medien, dann wird von externem „Whistleblowing“ gesprochen (Bürkle 2004: 2158).

Zum Vergleich: Der Schutz des Whistleblowers in den Vereinigten Staaten erfolgt auch in den öffentlichen und politischen Sektoren. Hier lösten große politische Skandale (zum Beispiel die „Pentagon Papiere“ oder die Watergate-Affäre) die Entwicklung des Whistleblowerschutzes aus (Groneberg 2011: 76). Während also dort der Whistleblower auf Schutzgesetze und eine positive Grundstimmung stößt, die durch zahlreiche Interessengruppen und gemeinnützige Organisationen noch unterstrichen wird, wandelt sich hierzulande das öffentliche Bild vom Whistleblower nur langsam (Deiseroth/Falter 2014). Veränderungen zeigen sich vor allem im Bereich der Unternehmen. Die Amerikaner definieren den Whistleblower nicht als Verräter, sondern als Informationsquelle: Er kann Informationen über Problemlagen liefern und so die Effizienz oder die Reputation des gesamten Betriebes verbessern (Röhrich 2008: 26; Wyler 2013). Die Geschäftsleitung zieht internes „Whistleblowing“ vor, um Imageschäden zu vermeiden. Den Arbeitnehmer kann dieser Umstand in eine Zwickmühle bringen. Die Schwere der aufzudeckenden Tat verlangt daher vom potenziellen „Verräter“ eine Abwägung, wie sie sonst nur Arbeitsrichter vorzunehmen hätten (Deiseroth 2008: 251).

Die Enthüllungen Edward Snowdens im vergangenen Jahr haben weltweit eine gewaltige Überwachungsdimension offengelegt. Snowden stellt eine Zäsur in der Geschichte der Whistleblower dar und muss daher als Super-Whistleblower bezeichnet werden. Viele Hacker, die vorher als paranoid galten, fühlen sich nun durch ihn bestätigt. Sein Geheimnisverrat hat das Vertrauen in die digitale Kommunikation grundsätzlich erschüttert. Die Töne innerhalb der Netzgemeinde sind seitdem spürbar radikaler geworden, denn die Erkenntnis reift, dass nur noch zwei Optionen bleiben: Entweder schränken sie ihr Kommunikationsverhalten durch rigide Verschlüsselung ein (Abwehr) oder sie üben digitalen Ungehorsam aus und gehen in die Offensive.

Digitale Selbstverteidigung ist freilich nur der erste Schritt: Eine wirkungsvolle Agenda der Regierungen lässt auf sich warten. In diesem Zusammenhang ist die Bürgersouveränität, zu der die Datensouveränität gehört, aufs Neue gefordert, und zwar sowohl hinsichtlich der liberalen „privacy“ wie der demokratischen Kontrolle von Regierungen und Internetkonzernen. Die Impulse müssen von Menschen ausgehen, die selbstbestimmte Bürger bleiben und wieder werden wollen. Das wirklich Neue im digitalen Zeitalter ist die Überwachung von Meta-Daten. Nicht länger interessieren die konkreten Inhalte, sondern die Muster und Strukturen der Kommunikation. Unsensible Daten wird es nicht länger geben, wenn es sie je gegeben hat.

3 | Anonymous-Bewegung

Wie schon der Name Anonymous verrät, wollen die Aktivisten dieser Bewegung unentdeckt bleiben. Sie übernehmen die Rechnersysteme von Großkonzernen, blockieren Websites und verlangen vollständige Freiheiten für das Internet. Während sich viele Menschen mit ihnen auf Demonstrationen solidarisieren und deshalb die zum Symbol für den Protest ge-

wordene Guy-Fawkes-Maske tragen, darf trotzdem angenommen werden, dass es nur wenige Spezialisten gibt, die das Knacken von Firewalls bestimmter Regierungs- und Unternehmensseiten beherrschen. Daher ist Anonymous keine Gruppe, sondern eher eine Idee (Reißmann u. a. 2012: 8), der man anhängt. Die Aktivisten nutzen Pseudonyme, treffen sich in Chaträumen und arbeiten dort an Manifesten. Bruchstücke solcher Arbeiten finden sich zum Beispiel in schlagkräftigen Kurzsätzen auf der Hauptseite der deutschen Anonymous-Bewegung. Wo es zum Beispiel heißt: „Wir wollen wissen, was wahr ist", „Wir diskutieren, wir artikulieren und wir akzeptieren, was wir für wichtig halten" und „Alles ist erlaubt" (Anonymous 2013). Das klingt anarchisch und durchaus problematisch im politischen Raum. Tatsächlich gibt es eine neue Aktualität des Anarchismus. Ohne Ideologie und spielerisch, ohne die Konsequenzen des eigenen Handelns zu bedenken, wird der Anarchismus neu ausprobiert, wozu das Netz geradezu einlädt. Eine neue Generation wird dies nutzen.

Ihren Anfang nahm diese Bewegung auf der Internetwebseite 4chan.org. Nutzer können dort Texte oder Bilder ungefiltert online stellen. Am 15. Januar 2008 öffnet hier der Nutzer „Anonymous" ein Unterforum mit dem Titel „Project Chanology". Der erste Teil von „Chanology" spielt auf die Hauptwebsite 4chan.org an, der zweite Teil auf die Sekte Scientology – das erste erklärte Ziel der Hacker-Vereinigung. Die Kommentatoren verlangen, dass die offizielle Scientology-Webseite „ausgeschaltet" werden soll (Reißmann u. a. 2012: 58). Drei Tage nach der Erstellung des Unterforums auf 4chan.org war die Scientology Webseite nicht mehr zu erreichen. Der Grund war eine Denial-of-Service-Attacke (DDoS).

Nach den Ereignissen um Wikileaks und der Ankündigung der Kreditkartenfirmen Visa Inc. und Mastercard Incorporated, die geleisteten Spenden an das Whistleblower-Netzwerk nicht auszubezahlen, sowie jede Geschäftsbeziehung mit Julian Assange zu unterbinden, wurde die „Operation Paypack" geboren. Dahinter stand ein loser Zusammenschluss anonymer Internet-Aktivsten, die sich zuvor über 4chan.org kennengelernt hatten. Eine kleine Gruppe von Hackern koordinierte die Aktion. Die Webseiten von Visa Inc. und Mastercard Incorporated sowie der Zahlungsverkehr über ihre Internetpräsenz wurden daraufhin das Ziel einer DDoS-Attacke. Stundenlang sollten diese am 7. Dezember 2010 nicht erreichbar sein (Janssen 2011). Selbst Webseiten von Regierungen, Parteien und Präsidenten wurden Opfer solcher Angriffe. Anlässlich der Blockupy-Proteste im Jahr 2012, deren Anhänger ihre Zelte im Frankfurter Rebstockpark aufstellten, geriet auch die Webseite der Stadt Frankfurt unter den Druck massiver Serveranfragen, der sie am Ende nicht standhielt. Eine Aktion, die für die Verschmelzung der Anonymous- und Occupyproteste steht (Reißmann u. a. 2012: 259), von deren Art sicherlich weitere folgen werden.

Die Leitidee hinter der Anonymous-Bewegung kann mit der Frage „Wie kommt die Zivilgesellschaft in die digitale Offensive?" beschrieben werden. Oft werden dabei Aktionen gewählt, die Kontrollverlust auslösen sollen, um zunächst schlichtweg zu sehen, was danach passiert.

4 | Internet-Aktivist Julian Assange

Der 1971 in Australien geborene Julian Assange gilt als Prototyp eines Internet-Aktivisten. Schon 1987 wählte er sich zum ersten Mal in das Internet ein und gab sich das Hacker-Pseudonym „Mendax" (lateinisch für Lügner). 2006 gründete er mit Mitstreitern die Enthüllungsplattform Wikileaks. Zwei Jahre später deckte das Netzwerk den Geldwäsche-Fall der Schweizer Bankengruppe Julius Bär auf. Wikileaks und Julian Assange wurden dadurch einer größeren Öffentlichkeit bekannt. Assange nutzte diese neue Aufmerksamkeit und intensivierte die Kooperation mit Journalisten. Es ging ihm fortan nicht nur um die bloße Bereitstellung brisanter Informationen, sondern er wollte die

Neuigkeiten auch ins rechte Licht gerückt sehen (Domscheit-Berg 2011: 40). Die Veröffentlichung eines Videos im April 2010 verdeutlicht dies. Das Ausgangsmaterial wird vor der Bereitstellung gekürzt sowie mit Kommentaren und Untertiteln versehen. Das Video zeigt den Angriff eines US-Kampfhubschraubers auf Bagdad. In den darauffolgenden Jahren kommt es zu weiteren Enthüllungen, in dessen Zentrum die Vereinigten Staaten stehen (Manne 2011), zum Beispiel die Veröffentlichung von Depeschen US-amerikanischer Botschaften im November 2010.

Julian Assange zeichnet sich durch eine spezielle Haltung zur Hacker-Gemeinschaft aus. Die von Wau Holland maßgeblich mitverfasste „Hackerethik" (Holland 1984) war für ihn nicht von Bedeutung. Der ehemalige Wikileaks-Mitstreiter Daniel Domscheit-Berg bemerkt, dass „selbst Hacker, die besondere Fähigkeiten hatten, (...) in seinen Augen Idioten [waren], wenn sie diese Fähigkeiten nicht für ein übergeordnetes Ziel einsetzten" (Domscheit-Berg 2011: 24). Im August 2012 flüchtete Assange in die ecuadorianische Botschaft in London, da ein internationaler Haftbefehl seine Auslieferung nach Schweden verlangte. Aus diesem Exil heraus versuchte er weiterhin politische Botschaften zu verbreiten und Geldmittel für seine Wikileaks-Plattform zu sammeln. Assange steht zwischen originären Whistleblowern und Aktivisten, die sich der Anonymous-Bewegung zugehörig fühlen und im Geheimen für ihre Überzeugungen eintreten. Er gibt dieser Bewegung ein Gesicht und stellt damit eine Ausnahmeerscheinung innerhalb der vielfältigen Formen und Akteure des digitalen Ungehorsams dar. Diese Rolle ist zu beachten, wenn wir zivilen und digitalen Ungehorsam miteinander vergleichen.

5 | Kriterien und Typen zivilen Ungehorsams

Der Politiker und Kommunikationswissenschaftler Peter Glotz, der selber ein politisches Kommunikationstalent war, erklärte in seinem 1983 erschienenen Buch „Ziviler Ungehorsam im Rechtsstaat", dass die Bundesrepublik Deutschland zwar eine parlamentarische Demokratie, aber der Bürgerprotest nur ein „halb-legitimer Bestandteil unserer Verfassungswirklichkeit" ist (Glotz 1983: 9). Er beschreibt damit die bis heute anhaltende Diskussion um die Legitimität zivilen Widerstands, die sich in der bewussten Übertretung von Gesetzen aus Gewissensgründen manifestiert. Je besser begründet dieser Widerstand ist, desto legitimer ist er. Seit den 1980er Jahren hat er sich unstrittig und gleichermaßen umstritten (an den Grenzen der Legitimität von Mehrheitsentscheidungen oder advokatorisch für Rechte, die nicht repräsentiert sind) in Deutschland „eingebürgert". Insofern ist bürgerlicher Ungehorsam der treffende Ausdruck dafür (Dworkin 1984:337-363).

Insbesondere das Konzept des gewaltfreien Widerstandes hat sich zu einem wichtigen Element des Protestes entwickelt, das allerdings nicht inflationiert werden darf. Wir fragen uns deshalb: Ist digitaler Protest eine neue Form des Ungehorsams? Wie lässt sich diese Protestform in das Konzept des zivilen Ungehorsams einordnen? Welche moralisch-politischen Gründe für die Aktivisten sind denkbar und was heißt „zivil"? Das Zivile lässt sich nicht auf das Bürgerliche beschränken.

Ronald Dworkin, der liberale Rechtstheoretiker, unterscheidet drei Typen zivilen Ungehorsams (Dworkin 1986: 104-116). Für den ersten Typ ist die Selbstachtung ein zentraler Begriff. Der Ungehorsam zeigt sich unmittelbar und unaufschiebbar, da Gewissensgründe ein starkes Gewicht haben. Bei den Fällen des zweiten Typs wollen die Akteure eine bestimmte Politik rückgängig machen und eine neue Mehrheit dafür sensibilisieren. Der zivile Ungehorsam des dritten Typs wendet sich nicht ausschließlich gegen ein offenkundiges Unrecht, vielmehr handelt es sich um Gehorsamsverweigerer, die eine „offizielle Politik" ablehnen. Alle drei Typen sind abhängig von bestimmten Situationen und den sich daraus ergebenden Handlungsoptionen. Sie müssen im Einzelnen

und mit Urteilsfähigkeit im Konkreten diskutiert werden (Kleger 1993).

Während sich der traditionelle zivile Ungehorsam meist gegen ein offensichtliches Unrecht wendet, versucht der neue Ungehorsam den Kurs der politischen Entwicklung zu verändern. Daher ist diese Art von Widerstand nicht nur auf Öffentlichkeit angewiesen, sondern er schafft geradezu Öffentlichkeit. Dabei geht es um Sichtbarmachung und Thematisierung. Man wendet sich gegen Tabus und Geheimbereiche in Politik, Militär und Wirtschaft. Gleichzeitig werden die Medien kritisiert, weil deren Informationen zur Meinungsbildung nicht ausreichen. Dieser Ungehorsam ist Indikator für Zivilitätsdefizite (Kleger 1993: 434). Umgekehrt zeigt sich die Zivilität des Ungehorsams genau darin, dass er friedlich und öffentlich bleibt. Er bekommt Schwierigkeiten der Vermittlung, wenn die (aufklärende) Öffentlichkeit als Großsubjekt selber in einer Krise ist und zunehmend erodiert (Imhof 2011).

In demselben Maße führen zum Beispiel Whistleblower ihre Argumente für die Aufdeckung von Geheimnissen an und erhöhen durch diese Aktionen des Ungehorsams den Preis für eine bestimmte Politik. Der Blick der Öffentlichkeit soll auf einen ganz bestimmten Missstand gelenkt werden. Es geht nicht um eine Vermittlung oder um die Suche nach einer Strategie zur Beseitigung der Unrechtmäßigkeiten, sondern in erster Linie um eine Störung der Effizienz der Auswüchse, die durch große öffentliche Beobachtung erreicht wird. Natürlich ist nicht auszuschließen, dass auch interessenbezogene Motive eines Arbeitnehmers Gewicht bei einem Verrat von Betriebsgeheimnissen haben können, zum Beispiel, wenn in einem Betrieb gegen Schutzvorschriften systematisch verstoßen und damit Beschäftigte in Gefahr gebracht werden. Das altruistische Handeln von Whistleblowern steht aber im Zentrum der Betrachtung, denn sie wenden sich an die Öffentlichkeit, weil sie versuchen, ihr eigenes, als Fehlverhalten verstandenes Handeln, durch die Bekanntmachung zu entlasten (Schmitt 2003: 5). Es steckt somit oft eine politische Absicht hinter einer Veröffentlichung, verbunden mit eigenen Gewissenskonflikten.

Edward Snowden war sich der Gefahr für sich und seine Familie durchaus bewusst, als er daran ging, die Weitergabe streng geheimer Dokumente der National Security Agency (NSA) vorzubereiten. Gleichzeitig wollte er in keiner „Welt leben, in der alles, was ich sage, alles, was ich tue, jeder, mit dem ich mich unterhalte, jeder Ausdruck von Kreativität oder Liebe oder Freundschaft aufgezeichnet wird" (Harding 2014: 11). Der Hinweisgeber agiert dabei gewaltlos und aus Gewissensgründen heraus, *Gewissen* hat auch immer etwas mit *Wissen* zu tun.

„Whistleblowing" ist also neuer ziviler Ungehorsam, weil es öffentlich geschieht und dabei nicht nur einen gewöhnlichen Gesetzesbruch darstellt, sondern politisch motiviert ist, um eine interessierte Öffentlichkeit zu informieren. Dies wird deutlich, wenn bestimmte Beispiele von „Whistleblowing" in Deutschland genauer betrachtet werden: Der BSE- und der Gammelfleisch-Skandal zum Beispiel, aber auch die Enthüllung der internen Sanktionsquoten in den Arbeitsagenturen wurden von deutschen Whistleblowern aufgedeckt und weckten bei der zu informierenden Gesellschaft stets die Frage: Wollen wir das wirklich? Am Anfang steht die schlichte Enthüllung eines vorher geheimen Faktums, doch letztlich wird Aufklärung erreicht, deren erstes Ziel nicht gleich die Veränderung des enthüllten Umstandes ist, sondern zunächst lediglich die Thematisierung.

Auch den Protestakteuren der Anonymous-Bewegung geht es um die Erhöhung des Preises für eine bestimmte Politik. Nur, dass ihr Handeln nicht auf eine bestimmte einmalige Veröffentlichung brisanter Daten ausgerichtet ist, sondern in ein längerfristiges strategisches Konzept eingebettet wird. Die zahlreichen Positionspapiere und Stellungnahmen zeugen von dieser Ausrichtung. Das ist ein Programm des Ungehorsams, dessen konfliktstrukturierende Strategie den Preis der dargestellten Praxis erhöht (Kleger 2013: 188).

6 | Legitimität von Protestformen

Können die häufig von Anonymous-Aktivisten durchgeführten DDoS-Attacken wirklich noch als legitime Protestformen anerkannt werden? Handelt es sich nicht vielmehr um Computersabotage, die in Deutschland mit bis zu drei Jahren Haft geahndet wird? Womöglich lassen sich solche Maßnahmen eher mit Sitzblockaden vergleichen: Wenn Demonstranten auf Kundgebungen gegen rechtsradikale Parteien Zufahrtsstraßen durch eine Sitzblockade versperren, dann ist unsere Bereitschaft, diesen Vorgang als gerechtfertigten Ungehorsam anzusehen, im Allgemeinen hoch (Asmus 2013). Wenngleich es das Ziel solcher Blockaden ist, andere Demonstranten und ihre Meinungen und Informationen fernzuhalten.

DDoS-Angriffe haben das gleiche Ziel. Die sinnlosen Anfragen blockieren jeden weiteren Datenaustausch und verhindern so, dass Informationen fließen. Man kann sogar von einer virtuellen Sitzblockade sprechen (Brandstädter 2012). Die Dimension dieses Protests lässt uns aber skeptisch zurück. Schließlich sind solche Attacken, wie sie im Zuge der Angriffe auf Visa Inc. und Mastercard Incorporated durchgeführt wurden, mit weitreichenderen Auswirkungen versehen. Die Anonymous-Bewegung nimmt für sich in Anspruch, dass Unbeteiligte nie Ziel ihrer Attacken sein werden. Wenn der Zahlungsverkehr wichtiger Kreditkartenfirmen jedoch für Stunden lahmgelegt wird, dann kann nicht davon gesprochen werden, dass kein Unbeteiligter die Folgen der Aktion zu spüren bekommt. Die Folgenverantwortung, die zur politischen Ethik gehört, ist nicht im Blick.

Im Mai 2012 wurden die sensiblen Daten der Unterzeichner der Aktion „Wir sind Urheber" durch Anonymous-Aktivisten erst erbeutet und dann online gestellt. Geht es ihnen dabei um einen Akt der Transparenz oder gar um Diskursfähigkeit? Sorgen solche Aktionen nicht eher für die Einstellung einer jeden demokratischen Auseinandersetzung (Hanfeld 2012)? Denn niemand unterzeichnet mehr eine Petition, wenn er befürchten muss, dass Hacker danach seine persönlichen Daten ausspionieren. Die Deutungspalette der digitalen Aktivisten reichen hier vom radikalen Anarchisten bis hin zum Planer von virtuellen Sitzblockaden. Aufgrund der spezifischen Umgebung muss also von einem digitalen Ungehorsam gesprochen werden, weil das Internet eine neue globale und uneingeschränkte Art des Informationsaustausches darstellt. Damit geht einerseits der Verlust von nationalstaatlicher Souveränität einher, die ohnehin schon beschränkt und konstitutionell geteilt ist. Die Geheimdienste versuchen andererseits durch Überwachung und Kontrolle, die staatliche Souveränität im Internet fast unumschränkt wiederherzustellen. Die sogenannte Netzgemeinde will dagegen das Internet als offenen und transparenten Ort der Kommunikation erhalten.

Heutzutage bilden sich über Staaten hinweg Protestgruppen, die Demokratiedefizite thematisieren und eine Weltöffentlichkeit schnell und vergleichsweise kostengünstig erreichen. Whistleblower nutzen diesen Umstand und lenken mit ihren Enthüllungen die transnationale Aufmerksamkeit auf Enthüllungsereignisse. Auch die Anonymous-Bewegung und andere Internet-Aktivisten wie Julian Assange machen sich diesen Umstand zunutze. Hinzu kommt, dass Politik und Recht ein schrumpfendes Problemlösungsvolumen haben, sowie gleichzeitig die Zahl der Probleme zunimmt, die sie lösen sollen. An dieser Stelle kommt der digitale Ungehorsam zum Tragen. Die digitalen Protestakteure versuchen, Probleme auf der politischen Prioritätenliste weiter nach oben zu verschieben: Enthüllungen, DDoS-Attacken und die Präsenz von Internet-Aktivisten lösen keine Probleme, sie dienen aber als hartnäckiger Indikator für dahinterliegende Defizite.

7 | Die Zukunft des digitalen Ungehorsams

Für Whistleblower kann die Annahme vertreten werden, dass sich aus ihren Bekanntmachungen häufig weitergehendes bürgerschaftliches Engagement entwickelt. Es werden breite Diskussionen geführt, Petitionen unterzeich-

net, Demonstrationen organisiert und politische Vorhaben artikuliert – allein aus dem Umstand heraus, dass die originäre Information erstmalig bereitsteht. Damit kann zwar nicht automatisch ein kausaler Zusammenhang zwischen der Enthüllung von Geheimnissen durch Whistleblower und der Steigerung politischen Engagements von Bürgern geschlossen werden. Es wird aber deutlich, dass Whistleblower aufgrund der schieren Möglichkeiten des Internets politische Akteursqualitäten im Sinne eines neuen Ungehorsams für die heutige Weltöffentlichkeit erlangen.

Kritischer zu sehen ist dieser Zusammenhang bei Aktionen der Anonymous-Bewegung und bei Aktivisten wie Julian Assange. Diese Aktionen lassen eine Vielzahl von ernsthaften Widersprüchlichkeiten entstehen. Sie wollen Menschen nicht nur informieren, sondern ihre vermeintlichen Gegner auch bestrafen. Veröffentlichungen erhalten somit den Charakter eines digitalen Prangers. Im Fall der Anonymous-Bewegung liegt dies an ihrer Nicht-Struktur; im Fall von Julian Assange an seinem übersteigerten Ansatz. Anders als Whistleblower können diese beiden Protestaktivisten nicht eindeutig einem neuen digitalen Ungehorsam im zivilen Sinne zugerechnet werden, der darüber hinaus zur Belebung einer demokratischen Protest- und Diskussionskultur beiträgt. Das Risiko unbeherrschter Angriffe ist bei beiden zu groß. Das *Risiko*, für das man selber einzustehen hat, wird damit zu einer ernsthaften *Gefahr* für andere, was sich moralisch nicht verantworten lässt.

Die Züge des Klandestinen und Konspirativen widersprechen zudem den Kriterien des zivilen Ungehorsams. Hier manifestiert sich ein Unterschied in der Veröffentlichungspraxis von Edward Snowden und Julian Assange: Während Assange auch Listen mit Klarnamen, zum Beispiel von Botschaftern und Agenten, ins Netz stellte, versuchte Edward Snowden in Zusammenarbeit mit Glenn Greenwald und Laura Poitras, solche Informationen erst schrittweise an die Öffentlichkeit zu geben, damit sie journalistisch verantwortungsvoll bearbeitet werden konnten (Greenwald 2014). Diese Nuance im Konkreten zeigt, dass diesseits der legalistischen Kritik am Widerstandsrecht (in der Tradition von Kant) die *Zivilität* des Ungehorsams möglich ist.

Die „!Mediengruppe Bitnik" aus Zürich verfolgt einen anderen Weg und verknüpft so den zivilen mit dem digitalen Ungehorsam. Ihre „Opera Calling Aktion" bezieht sich direkt auf die sogenannten „Opernhauskrawalle" Anfang der 1980er Jahre („Züri brännt"). 30 Jahre später steht wiederum die Kritik an der hochsubventionierten Hochkultur Zürichs im Mittelpunkt. Diesmal kommt es jedoch zu heimlichen Ungehorsamsaktionen. Das Opernhaus der Stadt wird verwanzt und an den Wanzen befestigte Mobiltelefone rufen zufällig Einwohner von Zürich an. Sobald der Telefonhörer abgenommen wird, schalten sich die Wanzen live und alles, was im Opernhaus geschieht, wird übertragen. Weitere Aktionen der „!Mediengruppe Bitnik" liefern erfindungsreiche Beispiele für kreative Umgangsformen mit kritischen Themen der „Digital Natives". Sie dringen zum Beispiel in verschiedene Überwachungssysteme ein, um mit dem Sicherheitspersonal auf ihren Überwachungsmonitoren Schach zu spielen.

2011 verschickten die Aktivisten sogar ein Paket an Julian Assange in die ecuadorianische Botschaft nach London. Im Paket befand sich eine aktivierte Kamera, die durch ein kaum sichtbares Loch fast sekündlich Bilder schoss und diese dank eines Mobiltelefons an eine Webseite und den Kurznachrichtendienst Twitter schickte. Immer gingen diese Aktivitäten der Frage nach: Wie sicher sind unsere Kommunikationswege? Die Systeme werden künstlerisch umgenutzt, wodurch Kritik an der Überwachung und der Einschränkung von Rechten geübt wird. Dies ist eine Möglichkeit, den digitalen Ungehorsam spielerisch zu gestalteten. In der modernen Kunst ist vieles erlaubt, was in der demokratischen Politik nicht geht. Diese Unterscheidung sollte man im Auge behalten. Deswegen sollten Kritik und Metakritik beachtet werden.

Die rechtliche Situation von Angriffen auf Überwachungssysteme und Serverdienste ist zumindest in Deutschland eindeutig. Nach deutschem Recht stellen die DDoS-Attacken eine Straftat dar. Der Paragraph 303b des Strafgesetzbuches verbietet die erhebliche Störung fremder Datenverarbeitungen ausdrücklich (§ 303b StGB). Eine Schlussfolgerung für die politische Theorie lautet deshalb: „(...) cyberprotest is cheap, digital disobedience easy. Democracy and the rule of law, however, are difficult and hard-won" (Baggini 2011). Darum sind auch die Anforderungen an den zivilen Ungehorsam als *Ausnahme* – und nicht als *Regelmethode* der Demokratie – hoch. In der Regel geht es um Mehrheitsbildungen.

Präsident Obama forderte in einer Rede Anfang des Jahres 2014, dass das Recht auf Privatsphäre zum „Weltrecht" erhoben werden soll. Edward Snowden war sich der hart umkämpften Errungenschaften des Rechtsstaats und der Demokratie durchaus bewusst. Er verteidigte bei jeder Gelegenheit den vierten Zusatzartikel der amerikanischen Verfassung, das Schutzrecht vor staatlichen Übergriffen (Harding 2014: 123). Snowden kann als Verfassungspatriot im amerikanischen Sinne bezeichnet werden. Jedoch haben weder die Verfassung noch die Möglichkeiten der Whistleblower-Schutzgesetze in den Vereinigten Staaten es ihm gestattet, innerhalb des Systems Kritik zu üben. Nur der digitale Ungehorsam hat ihm das ermöglicht.

Heinz Kleger ist Professor für Politische Theorie an der Universität Potsdam. Kontakt: kleger@ uni-potsdam.de

Eric Makswitat promoviert an der Universität Potsdam zum Thema: Big Data als Risiko für den „digitalen Ungehorsam". Kontakt: eric.makswitat@uni-potsdam.de

Literatur

Anonymous 2013: Du bist Anonymous. Abrufbar unter: http://du-bist-anonymous.de/freiheit.html, letzter Zugriff am 12.06.2014.

Asmus, Heilgard (Hg.) 2013: Rechte Aufmärsche und demokratische Proteste in Brandenburg. Potsdam.

Baggini, Julian 2011: Cyber-Protest is Cheap, Digital Disobedience Easy: The Dangers of Digital Disobedience. In: Literal Magazine, Abrufbar unter: http://www.literalmagazine.com/english_post/cyber-protest-is-cheap-digital-disobedience-easy-the-dangers-of-digital-disobedience/, letzter Zugriff am 12.6.2014.

Barlow, John Perry 1996: A Declaration of the Independence of Cyberspace. Abrufbar unter: https://projects.eff.org/~barlow/Declaration-Final.html, letzter Zugriff am 12.06.2014.

Brandstädter, Dietmar René 2012: Anonymos Aufruf: DDOS Angriffe als Ausdruck zivilen Ungehorsams – für ein freies Internet, gegen Zenzur. In: humanicum. Abrufbar unter: http://humanicum.wordpress.com/2012/05/08/anonymous-aufruf-ddos-angriffe-als-ausdruck-zivilen-ungehorsams-fur-ein-freies-internet-gegen-zenzur/.

Bürkle, Jürgen 2004: Weitergabe von Informationen über Fehlverhalten in Unternehmen (Whistleblowing) und Steuerung auftretender Probleme durch ein Compliance-System. In: Der Betrieb, Ausgabe 40, 2158–2161.

Bug, Arnold/Beier, Diana Maria 2009: Whistleblower – Hinweisgeber mit Zivilcourage. Abrufbar unter: https://www.bundestag.de/blob/190436/2e01b3a139c2843f2d370f2f6a153323/whistleblower-data.pdf, letzter Zugriff am 12.06.2014.

Critical Art Ensemble (Hg.) 1998: Digital resistance: explorations in tactical media. New York, London.

Deiseroth, Dieter 2008: Whistleblower und Denunziatoren. In: Zeitschrift für Rechtspolitik, Heft 8, 248–251.

Deiseroth, Dieter/Falter, Annegret (Hg.) 2014: Whistleblower in der Sicherheitspolitik, Berlin.

Domscheit-Berg, Anke 2014: Mauern einreißen. Weil ich glaube, dass wir die Welt verändern können. München.

Domscheit-Berg, Daniel 2011: Inside WikiLeaks: Meine Zeit bei der gefährlichsten Website der Welt. Berlin.

Dworkin, Ronald 1984: Bürgerrechte ernstgenommen. Frankfurt am Main.

Dworkin, Ronald 1986: A Matter of Principle. Oxford.

Glotz, Peter (Hg.) 1983: Ziviler Ungehorsam im Rechtsstaat. Frankfurt am Main.

Greenwald, Glenn 2014: Die globale Überwachung: Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. München.

Groneberg, Rut 2011: Whistleblowing: Eine rechtsvergleichende Untersuchung des US-amerikanischen, englischen und deutschen Rechts unter besonderer Berücksichtigung des Entwurfs eines neuen § 612a BGB. Berlin.

Hanfeld, Michael 2012: Urheber-Appell Die schwarze Liste von Anonymous. In: FAZ.NET, abrufbar unter: http://www.faz.net/aktuell/feuilleton/debatten/urheberrecht/urheber-appell-die-schwarze-liste-von-anonymous-11750188.html, letzter Zugriff am 12.06.2014.

Harding, Luke 2014: Edward Snowden: Geschichte einer Weltaffäre. Düsseldorf.

Imhof, Kurt 2011: Die Krise der Öffentlichkeit: Kommunikation und Medien als Faktoren des sozialen Wandels. Frankfurt am Main.

Janssen, Jan-Keno 2011: Ionenkanonen gegen Wikileaks-Gegner. DDoS-Attacken: Ziviler Ungehorsam oder Straftatbestand? In: c't Magazin für Computertechnik Heft 1, 50–51.

Kleger, Heinz 1993: Der neue Ungehorsam: Widerstände und politische Verpflichtung in einer lernfähigen Demokratie. New York und Frankfurt am Main.

Kleger, Heinz 2013: Widerstand und ziviler Ungehorsam im demokratischen Rechtsstaat. In: *Enzmann, Birgit* (Hrsg.): Handbuch Politische Gewalt. Wiesbaden. 163–203.

Manne, Robert 2011: The Cypherpunk Revolutionary. In: The Monthly, abrufbar unter: http://www.themonthly.com.au/issue/2011/march/1324265093/robert-manne/cypherpunk-revolutionary, letzter Zugriff am 12.06.2014.

Reißmann, Ole/ Stöcker, Christian/ Lischka, Konrad, 2012: We are Anonymous: Die Maske des Protests – wer sie sind, was sie antreibt, was sie wollen. Hamburg.

Röhrich, Raimund 2008: Methoden der Korruptionsbekämpfung: Risiken erkennen – Schäden vermeiden. Berlin.

Schmitt, Bettina A. 2003: Whistleblowing – „Verpfeifen" des Arbeitgebers. Hamburg.

Holland, Wau 1984: Hackerethik, abrufbar unter: http://www.ccc.de/hackerethics?language=de, letzter Zugriff am 12.06.2014.

Wyler, Esther, 2013: Whistleblower – Verräter oder Hinweisgeber?, abrufbar unter: http://www.managementpraxis.ch/praxistipp_view.cfm?nr=4307, letzter Zugriff am 30.7.2013.

Lernprozesse beim Bürgerprotest gegen technische Großprojekte

Kann der Kampf gegen S 21 und für K 21 noch gewonnen werden?

Wolfgang Sternstein

Ein Kommentar zu Michael Wilk/Bernd Sahler (Hg.): **Strategische Einbindung**. Von Mediationen, Schlichtungen, runden Tischen ... und wie Protestbewegungen manipuliert werden. Edition AV, Lich/Hessen 2014, 14 Euro

Um mein Urteil gleich vorwegzunehmen: Dies ist ein eminent wichtiges Buch. Alle, die in Bürgerinitiativen und Sozialen Bewegungen tätig sind, sollten es gelesen haben, denn es schärft den Blick für die zahlreichen Fallgru-