Verschlüsselt, vernetzt, verletzlich – Aktivist_innen über Sichtbarkeit und Anonymität[1]

Kurzinterviews mit *Volker und Stefan*, *Antje Schrupp*, *Stephan Urbach* und *yetzt*

Jana Ballenthien/Alexander Hensel

Der Austausch von Bewegung und Forschung ist, so auch das Credo dieser Zeitschrift, elementar. Während Forscher_innen für Bewegungen Außenbeobachtungen, Detailanalysen oder historische Reflexionen zur Verfügung stellen können, profitiert auch Wissenschaft vom Austausch mit Aktivismus: Etablierte Perspektiven und Wissensbestände müssen überprüft, aktualisiert und weiterentwickelt werden, denn nicht selten hinkt Forschung den sozialen, politischen oder kulturellen Veränderungen aufgrund ihrer Produktionsbedingungen und Routinen schlicht hinterher. Dies gilt für Bewegung und Protest im Internet umso mehr, deren technische und kulturelle Entwicklungen sich oftmals rasant und schubhaft vollziehen, während soziale und politische Formationen im Netz nicht selten kurzlebig und fragil erscheinen.

Während in früheren Phasen der Netzkultur eher Potenziale und neue Möglichkeiten des Internets beschrieben wurden, stehen derzeit eher Herausforderungen und Probleme im Vordergrund (vgl. die Beiträge von Kathrin Ganz sowie Ulrich Dolata/Jan-Felix Schrape in diesem Heft), die sich sowohl aus Sichtbarkeit als auch aus Anonymität ergeben: Persönliche Verletzbarkeit, Wellen anonymer An- und Übergriffe von politischen Gegner_innen, die Erosion der Grenzen von Subkultur und Teilöffentlichkeiten, privatwirtschaftliche wie staatliche Überwachung oder gar politische Verfolgung. Die Umgangsweisen von Aktivist_innen mit diesen Herausforderungen der digitalen Sichtbarkeit, ihre konkreten Befürchtungen und Erfahrungen variieren jedoch erheblich.

Für uns als Forschende wirft das Phänomen der digitalen Sichtbarkeit nicht nur eine Reihe von inhaltlichen Fragen, sondern weist ebenso auf derzeit unbeantwortete Herausforderungen für die empirische Sozialforschung hin (vgl. den Beitrag von Ina Alber in diesem Heft). Vor diesem Hintergrund wurde bereits auf der diesem Themenschwerpunkt vorausgehenden Tagung „Politisches Handeln in digitalen Öffentlichkeiten – Grassroots zwischen Autonomie, Aufschrei und Überwachung", die im November 2014 in Göttingen stattfand, ein Austausch zwischen Forschung und Aktivismus organisiert.[2] Der damit begonnene Dialog soll hier in Form von Kurzinterviews mit Aktivist_innen weitergeführt werden, die aus unterschiedlichen inhaltlichen und politischen Perspektiven auf das Kontinuum zwischen Sichtbarkeit und Anonymität blicken.

Techniken der Unsichtbarkeit

Das Verhältnis von Protest und Bewegung zu Fragen von Anonymität und Datenschutz ist gelinde gesagt ambivalent: Obgleich sich beispielsweise in linksautonomen Bewegungen eine gewisse Tradition des Selbstdatenschutzes findet (vgl. den Beitrag von Carsten Ochs in diesem Heft), werden damit verbundene Forderungen und Ansprüche im aktivistischen Alltag oftmals vernachlässigt oder bewusst ignoriert,

um von etwaigen Potenzialen digitaler Kommunikation stärker profitieren zu können. Volker und Stefan*, privat wie beruflich in die Netzkultur involviert und seit rund zwanzig Jahren in Bürgerrechtsbewegungen aktiv, bringen die Probleme der gelebten digitalen Bequemlichkeit auf den Punkt.*

Stefan und Volker, ihr engagiert euch in der Krypto-Bewegung. Was ist das überhaupt und was macht ihr konkret?
„Krypto-Bewegung"? Keine Ahnung was das ist... Sollte es eine „Bewegung" geben, kennen wir sie nicht und sind auch kein Teil davon. Krypto ist, gerade gesellschaftlich gesehen, eher ein Randthema und weit von einer Bewegung entfernt. Wir kennen und nutzen aber seit den Anfängen Computer und das Netz, sind auf der einen Seite neugierig auf die tollen Möglichkeiten, sehen aber auch die Gefahren der deutlich einfacheren Überwachung und Kontrolle. Wir machen uns also Gedanken darüber, wie sich elektronische Medien wie Mail, Usenet oder Chats sowohl für lokale wie auch überregionale linke Gruppen und Aktivitäten verwenden lassen und versuchen unser Wissen zu teilen. Das Hauptaugenmerk liegt dabei auf der Frage, wie sich über solche Kanäle eine vor Abhören „sichere" Kommunikation erreichen lässt und wie beziehungsweise unter welchen Voraussetzungen sich die jeweilige Technik auch für klandestine Zusammenhänge eignet. Im Gegensatz zu der amerikanischen Tradition der Cypherpunks[3] sehen wir uns weder als „Technik-Nerds" (auch wenn Stefan an einer Linux-Oberfläche für die Verschlüsselungssoftware PGP mitprogrammiert hat) noch als Anhänger eines politischen Libertarismus.

Ihr bietet schon länger Verschlüsselungs-Workshops für Aktivist_innen aus ganz verschiedenen Bereichen an. Wie steht es denn generell um deren „Kryptokompetenz"?
In politischen Kreisen treffen wir in der Regel auf Menschen, die sich sowohl der möglichen Gefahr, als auch der Notwendigkeit zu verschlüsseln bewusst sind. Gewünscht wird sich dann aber die Diskette (früher), der USB-Stick (heute) mit einem oder zwei Programmen, die den Rechner sicher machen. Das gab es nie und wird es nie geben. Um zu verstehen, wie bestimmte Kommunikationsformen technisch funktionieren, mit welchen Werkzeugen man die Vertraulichkeit der Daten sicherstellen kann, worauf man dabei achten muss und was man auf keinen Fall tun darf, ist einiges an Wissen notwendig. Und hier ist nicht nur das Vorwissen sehr unterschiedlich, sondern leider auch die Motivation, sich auf die teilweise komplexe Materie einzulassen. Dieses Wissen versuchen wir immer wieder leicht verständlich zu vermitteln. Die eigentlichen Werkzeuge zum Beispiel zur Mailverschlüsselung mit GnuPG (kostenlose Software mit offenem und dadurch transparenten Quellcode ohne Überwachungshintertürchen des/der Hersteller_in) sind in den letzten Jahren aber deutlich komfortabler geworden, da muss niemand mehr zu Kommandozeilen-Befehlen greifen. Trotzdem ist das Einrichten und konsequente Nutzen von Verschlüsselung in einer größeren Gruppe immer noch eine logistische Herausforderung, deshalb unterbleibt es oft aus Bequemlichkeit, wider besseres Wissen...

Der Schutz vor staatlicher Überwachung wird bislang vor allem individuell, also als „Selbstdatenschutz" betrieben. Müsste dieser nicht eigentlich kollektiv politisch geregelt werden?
Das ist eine spannende Frage. Wir erleben es immer wieder, dass politische Gruppen, gerade solche, die mit einer gewissen Repression rechnen, sich viele Gedanken um eine sichere Kommunikation machen. Die gleichen Menschen und Gruppen aber greifen, sobald die explizit politische Ebene verlassen wird, für ihre Kommunikation oftmals bedenkenlos auf Facebook & Co zurück und „übersehen" dabei, dass so ebenfalls sehr viele relevante Daten an die Überwachungsbehörden geliefert werden. Es geht also auch um die Frage „Was von mir will ich öffentlich machen, was will ich auf jeden Fall vertraulich halten und wo ist es mir egal?". Hier kann wohl nur „Selbstdatenschutz" greifen, diese Entscheidungen kann mir nie-

mand abnehmen oder für mich treffen. Und ohne ein gewisses Mindestmaß an individueller „Kryptokompetenz" sind alle Maßnahmen leicht zu unterlaufen oder auszuhebeln. Eine kollektive politische Aufgabe ist aber sicher, überhaupt erst mal ein Problembewusstsein zu schaffen, Angebote zum Kompetenzerwerb zur Verfügung zu stellen, die notwendige Technik zu entwickeln und vorzuhalten und auf die entsprechenden rechtlichen Rahmenbedingungen hinzuarbeiten. Die aktuelle Bundespolitik geht ja leider mit Vorratsdatenspeicherung, mangelhafter Kontrolle von Geheimdienstschnüffeleien und Diskussionen zum Verbot starker Verschlüsselung in genau die entgegengesetzte Richtung.[4] Umso wichtiger ist es, Initiativen wie digitalcourage, freiheitsfoo, freifunk und ähnliche zu unterstützen.[5]

Ambivalenz der Sichtbarkeit

Während an der Verbreitung und Weiterentwicklung von Möglichkeiten zur anonymen Kommunikation und des Datenschutzes gearbeitet wird, nutzen andere Aktivist_innen bewusst und offensiv die Vorteile und Potenziale digitaler Sichtbarkeit. Hiermit jedoch sind gerade in sozialen Netzwerken wie Facebook oder Twitter oftmals Probleme und Herausforderungen verbunden, wie beispielsweise Shitstorms oder persönliche politische Anfeindungen und Nachstellungen (vgl. die Beiträge von Magdalena Freudenschuss und Ricarda Drüeke in diesem Heft). Zu dieser Ambivalenz der Sichtbarkeit haben wir Antje Schrupp *befragt, die sich als Journalistin und Aktivistin in verschiedenen netzfeministischen Zusammenhängen engagiert.*

Antje, wie andere feministische Aktivist_innen bist du sehr präsent in sozialen Netzwerken. Welche Erfahrungen hast du dort gemacht?
Das Wichtigste ist für mich der Austausch mit Menschen, die an ähnlichen Themen interessiert, aber in anderen Szenen und Kontexten zuhause sind. Dabei lerne ich viel Neues und bekomme Debatten mit, die ansonsten vielleicht an mir vorbeigegangen wären. Das Internet ermöglicht es ja, mit viel mehr Menschen in Kontakt zu sein, als es über Mail oder persönliche Begegnungen möglich war und ist. Insofern erweitert es meinen Horizont. Außerdem diskutiere und argumentiere ich gerne. Kommentardebatten in meinem Blog machen mir Spaß, aber genauso „Nebenbei-Diskussionen" auf Twitter und auf Facebook, wenn ich gerade Zeit und Lust dazu habe.

Welche Stärken resultieren deiner Meinung nach daraus, im netzfeministischen Diskurs so sichtbar zu sein?
Zum einen bedeutet es für mich, dass mich interessante Informationen, Projekte und Ereignisse tatsächlich erreichen. Auch weil Leute mir inzwischen aktiv Links schicken oder mich auf Sachen hinweisen, von denen sie wissen, dass es mich interessiert. Super finde ich es zum anderen auch, Positionen und Ansichten kontextbezogen in den Diskurs einzubringen. Wenn gerade alle über ein Thema reden und ich sage etwas, das ich von meinem feministischen Hintergrund her daran wichtig finde, bekommt das natürlich eine größere Aufmerksamkeit, als wenn ich ohne bestimmten Anlass einfach mal einen theoretischen Text schreibe. Es geht im Internet nicht nur um „Content", sondern immer auch um „Kontext", das heißt, theoretische Überlegungen, konkrete Ereignisse und persönliche Standpunkte kommen zusammen. Genau das ist übrigens schon immer die Praxis der Frauenbewegung, von daher gefällt mir das.

Welche Strategien nutzt du, um mit Anfeindungen und Verletzbarkeiten umzugehen, die aus der Sichtbarkeit entstehen?
Der wichtigste Punkt ist meiner Ansicht nach, sich klarzumachen, wessen Meinung mir etwas bedeutet und wessen nicht. Man darf nicht zu viel auf die Zustimmung der „Vielen" geben, denn es geht bei inhaltlichen Debatten um Qualität und nicht um Quantität. Was die destruktiven Kommentare angeht, so braucht man einerseits ein dickes Fell, andererseits aber auch die Entschlossenheit, schnell zu entscheiden, worüber und mit wem man diskutieren

möchte und worüber und mit wem nicht. In meinem Blog sind die meisten Störer irgendwann von selbst weggeblieben, nachdem ich sie über lange Zeit konsequent gelöscht und absolut gar nicht auf sie reagiert habe. Das ist natürlich keine Garantie, nicht doch irgendwann bedroht und beschimpft zu werden. Ich glaube, wenn das passiert, ist es vor allem wichtig, gut vernetzt zu sein und sich auf einen Kreis von Freundinnen und Freunden stützen zu können, und zwar innerhalb und außerhalb des Netzes. Da ich schon älter bin, ist mein Vorteil vielleicht, dass das Internet nicht meine hauptsächliche politische Basis ist, sondern dass ich auch vorher schon gut vernetzt war. Viele meiner feministischen Freundinnen sind im Internet gar nicht anzutreffen. Das heißt, wenn „das Internet" mich morgen rausmobben würde, wäre ich nicht allein und müsste auch nicht bei Null anfangen. Ich glaube, das macht mich ein Stück gelassener, wobei ich es aber nicht wirklich beurteilen kann, weil ich einen sehr schlimmen Shitstorm, der echt an die Substanz geht, bisher nicht erlebt habe.

Staatliche Repression und Verfolgung

Die besonderen Herausforderungen der digitalen Sichtbarkeit entstehen oftmals erst aus der komplexen Dynamik zwischen individueller Sichtbarkeit, kollektivem Engagement und Vernetzung. Stephan "tomate" Urbach, *beruflich als Buchhalter in Hanau tätig, ehemaliges Mitglied der Piratenpartei und Teil der netzaktivistischen Gruppe Telecomix[6], unterstreicht die konkreten Gefahren von Sichtbarkeit im Kontext autoritärer Regimen sowie die individuelle Überforderung, welche aus einem intensiven transnationalen Aktivismus resultieren kann.*

Stephan, du hast sowohl im europäischen als auch arabischen Kontext Erfahrungen mit der Verletzbarkeit durch digitale Sichtbarkeit gemacht. Wo liegen hier konkrete Unterschiede?
Aus meiner persönlichen Erfahrung liegt der Unterschied vor allem in der staatlichen Repression und der Bedrohung für Leib und Leben von staatlicher Seite. In einigen repressiven Staaten der arabischen Welt bringt Sichtbarkeit die konkrete Gefahr, eingesperrt oder gar getötet zu werden – und zwar von staatlicher Seite. In meiner Wahrnehmung sieht es in Europa danach aus, als dass Repression gegenüber Aktivistinnen (und manchmal auch Aktivisten) eher von nicht-staatlicher Seite ausgeht: Maskulist_innen, Rassist_innen und ähnliches Pack warten nur darauf, dass sich aktivistisch arbeitende Personen exponieren um sie dann anzugreifen – online wie offline (vgl. den Beitrag von Magdalena Freudenschuss in diesem Heft). Wir wissen mittlerweile auch von europäischen Aktivist_innen, die in einige Länder dieser Erde nicht mehr einreisen sollten, da ihnen dort durch ihre aktivistische Arbeit in Europa konkrete Gefahr droht. Auf der anderen Seite tun sich europäische Staaten schwer, Aktivist_innen aus der arabischen Welt in Europa Schutz zu gewähren, wenn diese sich entscheiden, ihre Heimatstaaten zu verlassen.

Wenn du auf deine biographischen Erfahrungen mit digitalem Aktivismus zurückblickst, was würdest du Aktivist_innen empfehlen?
Als weißer Mann mit regelmäßigem Einkommen in Deutschland ist das natürlich recht leicht zu sagen: Auszeiten nehmen, Erholung einplanen, soziales Leben mit Menschen außerhalb des Aktivismus. Das funktioniert unter meinen Voraussetzungen. Betroffene, die aktivistisch arbeiten, können aber keine Auszeit nehmen: Der Kampf von Feministinnen, People of Color[7], Trans*Menschen und anderen, deren Aktivismus auch Überlebenskampf bedeutet, haben diese Möglichkeit einfach nicht. Ich kann nur hoffen, dass diese Aktvist_innen Unterstützung erhalten, um wenigstens zwischendurch in Räumen leben zu können, in denen sie nicht ihren täglichen Überlebenskampf kämpfen müssen und somit die Chance haben, wenigstens kurzzeitig Energie zu tanken.
Trotz allem: Wo liegen die positiven Aspekte eines großen Sichtbarkeitsradius?

Netzwerkeffekte und spontane Verknüpfungen mit anderen Aktivist_innen sind super. Sei es, um sich zu koordinieren oder aber um sich gegenseitig den Rücken zu stärken, wenn man von Gegner_innen des Anliegens angegriffen wird. Natürlich sorgt eine große Sichtbarkeit auch für eine breitere Streuung des Anliegens, für das aktivistisch gearbeitet wird, und spontane Meldungen von Menschen, die helfen wollen, sind keine Seltenheit. Aus Netzwerkeffekten ergeben sich viele Möglichkeiten für Vorträge, Diskussionsrunden und auch Interviews in der Tagespresse: alles Möglichkeiten, das Anliegen weiter zu befördern und Menschen dafür zu gewinnen. Sichtbarkeit ist ein Gewinn für die Sache, so lange die sichtbare Person nicht sich selbst, sondern die Sache in den Vordergrund stellt. Natürlich gehören die Person und die Sache immer zusammen, aber das ist ein nicht auflösbares Dilemma. Mit der Sichtbarkeit kommt auch Verantwortung für das Handeln in anderen Kontexten. Ich glaube aber, dass die Vorteile die Nachteile aufwiegen.

Strategien der Sichtbarmachung

Ein anders gelagertes Potenzial der Sichtbarkeit findet sich in einem noch recht neuen Bereich des Netzaktivismus, dem sogenannten Datenjournalismus. Hier geht es nicht um die Sichtbarkeit von Aktivist_innen, sondern um die Sichtbarmachung von Daten, die über Verknüpfungs- und Darstellungsstrategien in leicht verständliches, investigatives Wissen transformiert werden können. Der Berliner Aktivist yetzt *berichtet über diesen Ansatz, welcher von der Initiative Open Data City erfolgreich praktiziert wird.*[8]

Was tun Datenaktivist_innen und was ist das Besondere daran?

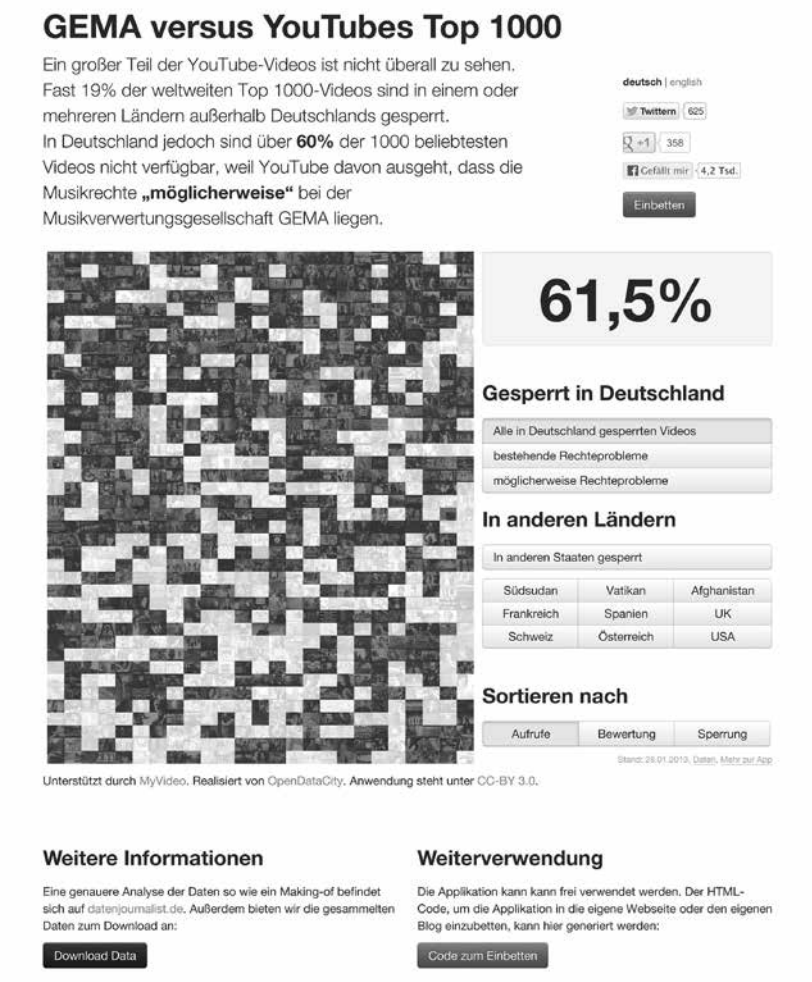
Datenaktivismus versucht, maschinenlesbare digitale Informationen zugänglich zu machen. Das kann auf viele Arten geschehen und hat unterschiedliche Aspekte. Es gibt zum einen den klassischen NGO-Aktivismus, bei dem es vor allem um die legale Offenlegung von Daten und die Aufklärung über offene Daten und freie Lizenzen geht. Dieser Aktivismus reicht von der Beratung von Unternehmen und nichtstaatlichen Organisationen zum Umgang mit Transparenz und offenen Daten, dem Lobbying für die Freigabe von privatisierten Datenhalden bis zum Erstreiten von Daten nach dem Informationsfreiheitsgesetz. Zum anderen gibt es Menschen und Organisationen, die für die direkte Verfügbarkeit von Daten sorgen, etwa durch Leaks, die Veröffentlichung von Daten nach Hacks oder das Programmieren von sogenannten Scrapern, die Daten aus öffentlichen, aber in ihrer Form kaum oder nicht nutzbaren Datenquellen zusammentragen, indem sie zum Beispiel automatisiert Websites kopieren.

Mal ganz konkret: Was ist ein typisches datenaktivistisches Projekt und wie wird hier genau Sichtbarkeit hergestellt?

Unser Vorgehen ist einfach. Wir veröffentlichen Daten, die entweder vorher schon zugänglich, in ihrer Form aber langweilig oder unverständlich waren (beispielsweise Datenkolonnen) oder aber erst auf Anfragen hin öffentlich gemacht werden. Wir bereiten diese dann verständlich auf. Unsere Ziele sind, etwas verständlich zu machen, was vorher nicht verständlich war; etwas sichtbar zu machen, was vorher nicht sichtbar war und damit neue Blickwinkel auf Themen zu schaffen. Manchmal nutzen wir die neuen Perspektiven auf Informationen, die sich ergeben, wenn Daten aus verschiedenen Quellen miteinander kombiniert werden. Durch die Aufarbeitung soll das investigative und gesellschaftlich relevante Potenzial der Daten freigesetzt werden. Ich nenne euch mal zwei typische Projekte. Das eine ist das Plagiatssuche-Portal Lobbyplag[9], das dokumentiert, wie häufig EU-Abgeordnete wörtliche Formulierungen von Lobbygruppen bei Datenschutzrichtlinien übernehmen. Als Datengrundlage nutzen wir dafür die Gesetzestexte, die zwar öffentlich sind, normalerweise aber nicht von vielen Menschen gelesen werden, und unveröffentlichte Lobbypapiere, die wir von uns positiv gesonnenen Parlamentarier_innen,

von NGOs und aus Leaks aus dem Internet zusammenstellen. Ein zweites schönes Beispiel ist unser Projekt zur Vorratsdatenspeicherung. Wir machten die von Providern gesammelten Daten, die ja Bewegungsprofile darstellen, in Karten sichtbar, um den Eingriff in die Privatsphäre zu verdeutlichen. Bekannt ist vielleicht das Bewegungsprofil des Grünen-Politikers Malte Spitz, in dem wir frei im Internet zugängliche Daten unter anderem mit den Geodaten seines Smartphones kombiniert haben.[10] Schön visualisieren lässt sich auch der Umgang von YouTube mit der Sperrung von Videos (Abb. 1). In einer interaktiven App haben wir die Top 1000 der

Abb. 1: GEMA versus YouTubes Top 1000 (Screenshot; gesperrte Videos dunkel hinterlegt)



Quelle: https://opendatacity.de/download/highres/gema_youtube/images/webpage_rank_de.png (CC-BY OpenDataCity; 26.08.2015).