

## Widerstände und neue Widerstands-Möglichkeiten

### Raus aus dem User Dasein!

Die Technokraten der IT-Offensive begnügen sich nicht mit der Entwicklung von Erfindungen, oder Techniken deren Anwendung oder Ablehnung sie den gesellschaftspolitischen Akteuren überlassen. Sie sorgen mit der Entwicklung eines technologischen Schubs für eine grundlegende Veränderung von Gesellschaft. Technologie macht damit in noch viel stärkerem Maße Politik als wir das bisher kennen.

Die Appifizierung des Sozialen gelingt nur deshalb so reibungslos, weil wir bewusstlos als Bequemlichkeits-verblendete „User“ mitmachen. Obwohl wir genau wissen und mittlerweile im Feuilleton täglich in die Augen gerieben bekommen, dass *Überwachung* nicht mal annähernd das beschreibt, um was es eigentlich geht: die beeinflussende Reorganisation unseres Denkens und Handelns.

Die vollständige Durchleuchtung unseres Tuns und Denkens ist dabei eher die Basis als das ganze Ausmaß des Übergriffs: Wer erhält welche Informationen, in welches Korsett zwingt sich Kommunikation - die Fremdbestimmung ist das entscheidende Merkmal dieses technologischen Umwälzungsprozesses. Befeuert wir diese Maschinerie derzeit durch ihren Hauptmotor – das BigData Business.

Wir fordern keine vollständige digitale Entsagung – das wäre Quatsch wir fordern aber ein redlicheres Abwägen zwischen der vermeintlichen Bereicherung versus Entmündigung und Entfähigung durch diese Technologie. Uns geht es nicht um das Heraufbeschwören einer unverfälschten, vermeintlich echten Sozialität mit Retro-Faktor ohne soziale Netzwerke und Smartphone. Uns wäre es sogar ziemlich egal, mit welchen schrulligen Erfindungen wir uns in einer befreiten Gesellschaft die Zeit vertreiben. Ganz und gar nicht egal ist uns die über diese Technologie erzeugte Ungleichheit, die rasant zunimmt und immer mehr gesellschaftlich Abgehängte und reichlich unsmart aus der Smartifizierung Entlassene produziert. Die Bedingungen für Befreiung werden ohne eine Abwehr des technologischen Angriffs deutlich schlechter. Da müssen wir den sogenannten *Akzelerationisten* entscheiden widersprechen. Die glauben in den gegenwärtigen Formen des kybernetischen Kapitalismus Kräfte zu erkennen, die zu seiner Überwindung hilfreich sein können.

Wir müssen raus aus der völlig unpolitischen Blindheit, diese lustigen Gadgets und unser Eingewoben-Sein ins Netz wären einfach nur eine Etappe eines „neutralen“ technologischen Fortschritts. Wir halten es für notwendig, uns gegenüber dem technologischen Angriff zur Wehr zu setzen, Widerstand zu organisieren und globale Player des Geschäfts mit der Entmündigung direkt anzugreifen. Wir müssen Möglichkeiten entwickeln ein kollektives Nein spürbar werden zu lassen.

Es wäre dringend nötig, ein solches Nein zu artikulieren z.B. gegenüber Amazon und dessen Verständnis von der uneingeschränkten Ausbeutbarkeit seiner Angestellten unter dem Kommando algorithmischer Optimierung der Arbeitsprozesse: Stellen wir uns vor, europaweit finden im Vorweihnachtsgeschäft Streiks in den großen Distributionszentren von Amazon statt. Die Zufahrtswege sind blockiert, LKWs kommen weder auf das Gelände noch können sie dieses verlassen. Auf einem Banner steht „We are not Machines!“ Kund\*innen unterstützen die Auswirkungen der Streiks indem sie vermehrt Bestellungen ab- und wieder retour-schicken und den Paketen solidarische Botschaften an die Belegschaft beilegen. Kundgebungen vor der Unternehmenszentrale, den Call Centern von Amazon und den neuen Innenstadt-Versandlagern in Berlin, München oder Dortmund treffen das Unternehmen sensibel: Wahrnehmbar schlechte Publicity und ernsthafte Störung der Zustellung, die so sehr auf Reibungslosigkeit „auf den letzten Metern“ setzt. Der Deutschland-Chef Ralf Kleber wird beim öffentlichen Auftritt getortet, die Homepage von Amazon gehackt. Selbst die Crowdfunding-Plattform von Amazon *mechanicalturk* für unterbezahlte Clickworker\*innen und entrechtete digitale Arbeitsnomaden hakt ...

Google kennt übrigens ein solches Nein, auch wenn Eric Schmidt als ehemaliger CEO keine politischen Gründe vermutet wenn er sagt: „Die Google-Unternehmenspolitik ist es, bis genau an die Grenze zu gehen, wo es den Leuten unheimlich wird, aber nicht darüber hinaus.“ Bei der Einführung von *google glasses* in den USA gab es einen solchen Moment – Die Dauerobservationsbrille mit Netzanbindung kam über eine kleine aber populäre und teils handgreifliche Kampagne gegen sogenannte *glassholes* in Verruf. Kneipen und angesagte Clubs untersagten das Tragen dieser filmenden Brille zum Schutz ihrer Kundschaft. Die Brille kam über die Auslieferung an Entwickler nicht hinaus und wurde vorerst eingestampft.

### Digitale Selbstverteidigung und befreite Software

Gibt es eine Option auf Autonomie, die sich eine »unabhängige« Nutzung von Technik erkämpft? Das ist zumindest die Zielsetzung eines großen Teils der Hackerbewegung. Die free software Bewegung, die deutlich über den zu kurz greifenden Ansatz des „open source“ Standards hinaus geht, sieht sich in dieser Tradition. Die

internationalen Kämpfe gegen Vorzugsbehandlung im Netz (Netzneutralität) und die Bemühungen um ausreichend starke Kryptografie gehören ebenso dazu.

Vermutlich würden ohne das von Aktivist\*innen entwickelte und besonders gesicherte Betriebssystem TAILS (The amnesic incognito live system) viele politisch Aktive den Verfolgungsbehörden ins Netz gehen. Das hält uns eine Weile über Wasser - immerhin hat selbst einer der am stärksten verfolgten, nämlich Edward Snowden in der Phase seines Abtauchens mit diesem Betriebssystem kommunizieren können ohne seinen Aufenthaltsort preiszugeben. Das sind notwendige, konstruktive Abwehrmaßnahmen gegen die Überwachungs- und Manipulations-Übergriffe von Staat und Tech-Industrien. Eine Bewegung, die sich um freie digitale Hard- und Software bemüht, ist absolut notwendig. Aber, sie ist absehbar nicht ausreichend angesichts der Massivität des technologischen Angriffs.

### **Technologie „hacken“**

Dazu noch einmal unser Beispiel von vorhin – die bevormundende Krankenversicherung, die unsere Alltagsbemühungen um ein gesundes Leben ausforschen und fremdbestimmen möchte: Einzelne Techniken können wir leicht „befreien“, sie ihrer ursprünglich zugedachten Bestimmung entreißen, sie „hacken“. Jedem würden auf Anhieb soziale „Hacks“ der zuvor erwähnten Fitnessarmbänder einfallen, die wir ganz ohne Programmierkenntnisse umsetzen könnten. Wir könnten damit erfolgreich unserer Krankenversicherung ein anderes Fitnessbemühen vortäuschen und den billigeren Tarif ergattern. Die gesellschaftliche Normierung über die Technologie, die auf „freiwillige“ Selbstoptimierung abzielt, würden wir damit aber nicht angreifen! Das ist ein wesentlicher Unterschied - Technologien zu hacken ist ein schwierigeres Unterfangen und setzt ein Bewusstsein für den technologischen Angriff nicht nur bei den Hackern sondern gesamtgesellschaftlich voraus. Deswegen brauchen wir auch eine diskursive Abwehr des technologischen Zugriffs weit über Methoden der Selbstverteidigung hinaus!

Es gibt jedoch auch neue Widerstandsformen, die wir aktiv und offensiv nutzen sollten. Ohne zu verkennen, dass die derzeitige „Nettobilanz“ im Widerstreit zwischen Bereicherung unserer Widerstandsoptionen versus Beschneidung unserer unkontrollierten Handlungsspielräume für den absolut überwiegenden Teil an Computer-Nicht-Expert\*innen eindeutig negativ ausfällt.

### **Whistleblowing**

Starten wir mit dem Whistleblowing – überhaupt keine neue aber eine neuerlich deutlich weiter verbreitete Widerstandsform. Sie ermöglicht Leuten zum politischen Subjekt zu werden, ohne sich offen zur Dissidenz bekennen zu müssen. Ich kann jahrelang im Apparat Informationen leaken, also raussickern lassen, ohne mich zu outen. Wir sollten diese Form noch populärer machen. Alle kennen Wikileaks, die meisten wissen aber nicht wie mensch einen wirklich anonymen Kontakt dorthin aufbaut. Der Heise-Verlag hat im Herbst 2016 eine weitere Plattform <https://heise.de/tippgeber> eröffnet, die es „Geheimnisträger\*innen“ leichter ermöglichen soll, anonym widerständig zu werden.

Wie bedrohlich der US-amerikanische Staat das Whistleblowing einstuft, sehen wir an der Haftstrafe von Chelsea Manning, die für 35 Jahre weggesperrt werden soll, sollte sie überhaupt so lange die folterähnlichen Haftbedingungen durchstehen. Wir sollten hier den Vorschlag einiger Computer-Aktivist\*innen aufgreifen und am 17.12. diesen Jahres – dem Geburtstag von Chelsea – einen Whistleblowing Aktionstag in vielen Städten machen. Hier könnten wir auf Veranstaltungen zusammen mit Queer- und Anti-Knast-Bewegung sowie Antimilitarist\*innen die Möglichkeiten und Limitierungen des *Leakens* diskutieren, praktische Anleitung geben, wie mensch sich via vorhin erwähntem TAILS anonym an eine solche Plattform wendet und wie wir Chelsea weiter unterstützen können.

### **Hacking**

Einen Schritt weiter gehen Hacker, beim Besorgen von Geheimnissen oder der Sabotage des politischen Gegners. Eine, oder mehrere Hacker\*innen, die sich *Phineas Fisher* nennen, haben eine der großen Cyberwaffenschmieden, die italienische Firma HackingTeam gehackt und alle Firmenmails und den Quellcode der Schnüffelsoftware offengelegt. Ein gigantischer Schaden, setzt die Schnüffelsoftware doch darauf unbemerkt von Virenprogrammen und sonstigen Sicherheitssystemen massenhaft Rechner zu befallen. Die gleiche Gruppe hatte zuvor auch den britisch-deutschen Trojanerhersteller FinFisher gehackt und bekannte sich auch kürzlich zum Klau und der Veröffentlichung von 300.000 emails der türkischen Regierungspartei AKP.

Detaillierte Erklärungen, wie die Hacker\*innen-Gruppe das angestellt hat, sollen als „Anleitung für alle, die nicht die Geduld haben, auf den nächsten Whistleblower zu warten“ dienen. In einem anonymisierten Interview hat sich Phineas folgendermaßen geäußert: „*Hacking gives the underdog a chance to fight and win*“.