2. Digitale Gegenökonomie

In Anlehnung an den Begriff einer Gegen-Identifikation von Pêcheux möchte ich im Folgenden den Begriff einer Gegenökonomie einführen, von der schließlich eine Desökonomie als weitere, aber andere Art, eine kritische Haltung zur digitalen Ökonomie einzunehmen, abzugrenzen sein wird. Wie die Gegen-Identifikation, so findet sich auch die Gegenökonomie in einer kontrollierten Symmetrie zur digitalen Ökonomie, die zumindest gewisse Annahmen, auf denen die digitale Ökonomie basiert (wie den Mehrwert von immer mehr Daten) unhinterfragt annimmt oder sogar noch bestärkt. Die Gegenökonomie konzentriert sich dabei vor allem auf das Konsumverhältnis von Nutzer*innen und lässt das Produktionsverhältnis außen vor, das heißt, sie stellt den *bewussten Konsument*innen bewusste Nutzer*innen* zur Seite. Dies zeigt sich insbesondere am sogenannten *Data Detox* der Gruppe Tactical Tech, dem ich mich im folgenden Kapitel widmen werde. Indem ich die Vorstellungen, die im Detox zum Tragen kommen, die antike Vorstellungen von Diät reaktivieren, im zweiten Kapitel auf die Schriften der Cypherpunks zurückverfolge, zeige ich, wie dabei Kontrolle und Souveränität der Nutzer*innen im Vordergrund stehen. Diese Vorstellungen werde ich im letzten Kapitel kritisieren.

2.1 Detox

Die Gegenökonomie teilt mit der digitalen Ökonomie die wesentliche Annahme, dass Daten wertvoll sind und stets eine Ressource darstellen, sodass eine Akkumulation von Daten einen Datenreichtum impliziert. Da die digitale Ökonomie auf dieser Ressource aufbaut, liegt der Schluss scheinbar nahe, darauf zu zielen, der Ökonomie diese Ressource zu entziehen. Die Gegenökonomie wendet sich dazu an die Nutzer*innen, die durch den Konsum von Diensten und Geräten Daten produzieren. Diese sollen nun aufhören zu konsumieren bzw. anders, das heißt bewusster, konsumieren, um letztendlich die digitale Ökonomie zu transformieren. Die Gegenökonomie läuft damit entlang ähnlicher Bahnen wie der Aufruf zu einem bewussten Konsum. Eine Definition des bewussten Konsums, die dies gut zeigt, lautet:

> Markt funktioniert so: Hier gibt es Angebote, dort gibt es eine Nachfrage, und irgendwo dazwischen treffen sich Konsumenten und Produzenten. Die Macht des bewussten Konsumenten liegt vor allem darin, Nein zu sagen zu schlechten Angeboten, dafür ausdrücklich Ja zu sagen zu besseren, also nachhaltigeren, umweltfreundlicheren oder ethischeren Angeboten.[1]

Was ist nun dafür nötig, um nach dem Modell der bewussten Konsument*innen das Ideal bewusster Nutzer*innen zu entwickeln? Unter Begriffen wie digitale Selbstbestimmung oder digitale Selbstverteidigung findet sich etwa: »Wissen wobei, wann und wo Daten erhoben und gespeichert werden«, »Solche Datenspuren vermeiden: Daten, die erst gar nicht erhoben wurden, können auch nicht missbraucht werden« und »Beim Websurfen [sich] nicht dauerhaft identifizieren und verfolgen lassen: Tracking erschweren und das Legen digitaler Krümelspuren abschalten«[2]. Bei netzpolitik.org gibt es ähnliche Tipps wie man »eigene Daten besser vor Facebook schützen« und »Google unter Kontrolle halten« kann oder die »eigenen« Daten zurückholt.[3] Für die bewusste Nutzung werden somit Mittel an die Hand gegeben, wie man den ›schlechten Angeboten‹ wie Facebook und Google Daten entziehen kann, und Alternativen aufgezeigt. Die entsprechenden Angebote informieren die Nutzer*innen, warum es eines bewussten Umgangs mit Onlinediensten bedarf und wie dieser aussieht. Bewusste Nutzung bedeutet dabei vor allem Kontrolle über die eigenen Daten zu erreichen, um auf diese Weise die digitale Ökonomie zu transformieren: weg von der Abhängigkeit von massiver Akkumulation von Daten hin zu Diensten, die Privatsphäre, Anonymität und Daten schützen. Wie es Guido Zurstiege in *Taktiken der Entnetzung* zusammenfasst: »Digitale Selbstverteidigung setzt […] einen aktiven Mediennutzer voraus, der über ein hinreichendes Problembewusstsein, aber auch über die entsprechenden Kenntnisse von Taktiken der digitalen Selbstverteidigung verfügt.«[4] Als Ideal (das normale Nutzer*innen nur in Graden erreichen würden) wird von Zurstiege ein technisch versierter Kollege angeführt, der unter anderem ein sogenanntes Blackphone besitzt. Dieses Produkt sei kaum zu knacken und sendet so wenig wie möglich Daten, sodass es sogar regelmäßig vom Mobilfunkanbieter als fehlerhaft fehldiagnostiziert wird, mit der Konsequenz, dass der Service

1 Andreas Winterer, »Die Welt verändern? Bewusster Konsum kann es schaffen!«, *utopia.de*, 9. April 2019, https://utopia.de/ratgeber/so-kann-bewusster-konsum-die-welt-veraendern/.

2 »Digitale Selbstverteidigung für Eilige«, zugegriffen 12. August 2018, https://selbstdatenschutz.info/digitale_selbstverteidigung.

3 Vgl. Alexander Fanta, Tomas Rudl und Ingo Dachwitz, »Kleines Einmaleins der digitalen Selbstverteidigung«, 30. April 2018, https://netzpolitik.org/2018/kleines-einmaleins-der-digitalen-selbstverteidigung/.

4 Guido Zurstiege, *Taktiken der Entnetzung: Die Sehnsucht nach Stille im digitalen Zeitalter* (Berlin: Suhrkamp, 2019), 124.

kurzfristig unterbrochen wird. Damit sei das Produkt und der Kollege, der diese Unbequemlichkeit in Kauf nimmt, um seine Privatsphäre zu schützen, vorbildhaft für das Konzept einer *Datensparsamkeit*: Mit diesem Konzept sind einerseits Produkte gemeint, die Daten im geringeren Maße sammeln bzw. weitergeben, sowie Nutzer*innen, die sich diesem Wert verschreiben. Es »gemahnt sie [die Nutzer*innen] an ihre Verantwortung, in der täglichen Nutzung dieser Technologien möglichst wenige, allenfalls nur die notwendigen persönlichen Informationen preiszugeben«[5].

Auch die Berliner Gruppe Tactical Tech verfolgt einen Ansatz von Aufklärung, der die Nutzer*innen an diese Verantwortung erinnern und entsprechende Wege aufzeigen soll. Bezeichnend ist dafür etwa das sogenannte *Data Detox Kit*, das damit wirbt, »[a]lltägliche Schritte [zu bieten], mit denen Du Deine digitale Privatsphäre, Sicherheit und Wohlbefinden kontrollieren kannst, und die zu Dir passen«[6]. Das *Data Detox Kit* wurde für die von Tactical Tech kuratierte und von Mozilla präsentierte Ausstellung *Glass Room* angefertigt, die 2017 in London stattfand. Darin werden eine Reihe von Maßnahmen erläutert, sowohl warum diese wichtig sind als auch wie man diese Schritt für Schritt umsetzt. Man kann zum Beispiel gewisse Einstellung ändern, die standardmäßig am Smartphone oder am Computer voreingestellt sind, alte Apps löschen und auf alternative Apps ausweichen oder Erweiterungen installieren, die Werbung und Cookies blockieren. Die Notwendigkeit eines bewussten Umgangs mit den eigenen Geräten und Diensten wird dabei wie folgt begründet:

> Wenn Du darüber nachdenkst, was Deine Daten anderen über Dich verraten, dann scheint es vielleicht keine große Sache zu sein: Wen interessiert es schon, ob Du gern Country-Musik hörst; […]? Das Problem ist, was mit Deinen Daten passiert. Über einen Zeitraum gesammelt **kommen intime digitale Muster zum Vorschein**: Deine Gewohnheiten, Bewegungen, Beziehungen, Vorlieben, Ansichten und Geheimnisse eröffnen sich denjenigen, die sie *analysieren und von ihnen profitieren*, wie Unternehmen und Datenbroker. Im Verlauf dieses Daten-Detox erhältst Du einen Einblick, wie und warum all das passiert, und ergreifst praktische Maßnahmen, um **Deine Datenspuren im Internet zu kontrollieren**.[7]

Der bewusste Umgang wird somit einerseits als nötig dargestellt, um die *eigene* Privatsphäre zu schützen, stellt mithin eine Praxis zum Selbstschutz dar – entgegen meiner Argumentation zur algorithmischen Gouvernementalität, die nicht ›intime Muster‹ problematisierte, sondern Muster innerhalb von Daten-Nachbarschaften. Wie Pepita Hesselberth resümiert, werden dadurch andererseits die nicht-bewussten Nutzer*innen stigmatisiert: Die Nutzer*innen selbst seien letztendlich das Pro-

5 Zurstiege, 128.

6 »Data Detox Kit«, zugegriffen 14. April 2023, https://datadetoxkit.org/de/home.

7 »Kontrolliere Deine Smartphone-Daten«, zugegriffen 14. April 2023, https://datadetoxkit.org/de/privacy/essentials/ [Herv. i.O.].

blem, insofern sie nicht bewusst konsumieren und damit all die Standardeinstellungen übernehmen. Denn indem Hesselberth der Frage nachgeht, für wen die Notwendigkeit eines Detox besteht und was damit als toxisch verstanden wird, landet sie bei den Technologien selbst, die von einem falschen Konsum gereinigt werden müssen: »it now turns out to be ›you‹ who is clogging up the system by sharing all of your thoughts, ›habits, movements, connections, beliefs, secrets and preferences online.‹ In other words: your digital footprint – not ›big data‹ and not even ›toxic tech‹ as such – is here envisioned to be toxic.«[8] Beispielhaft zeigt sich das etwa unter der Anleitung zur App-Entrümpelung. Dort wird der Exzess an Daten, die Apps auf dem Smartphone produzieren, implizit mit einem Konsum verbunden, bei dem man gar nicht mehr weiß, was all die Anwendungen machen, die man irgendwann mal installiert hat: »If you've ever been scrolling through your apps and wondered ›When did I download this?!‹ or ›What does that even do?‹, this is for you.«[9] Die so entstehende Ansammlung von Daten wird als »*your* data bloat«[10] bezeichnet; eine Datenaufblähung, die den Nutzer*innen zuzuschreiben ist. Es sind die Nutzer*innen, die durch ihr Verhalten die Datenaufblähung verursachen, die durch einen nicht-bewussten Konsum dazu beitragen, dass zu viele Daten produziert werden – ich komme darauf im Kapitel zu *Clicks* und dicken_fetten Daten (3.2.1) zurück.

Wie es an anderer Stelle suggeriert wird, sind die Nutzer*innen damit dem Sog, den Geräte und Dienste entwickeln, verfallen und müssen nun lernen, sich davon zu befreien. Es heißt entsprechend weiter: »Vielleicht wirst Du es nicht glauben, aber Deine Lieblings-Apps und -Webseiten sind so designt, dass jede Funktion, jede Farbe und jeder Ton dazu ›optimiert‹ wurde, Dich zu fesseln, zu überzeugen und immer wieder nach dem Handy greifen zu lassen.«[11] Damit verbindet sich zuletzt der *Data Detox* mit dem *Digital Detox*, der nicht nur von der Produktion von Daten, sondern von der Abhängigkeit vom digitalen Milieu insgesamt befreien möchte. Zu dem Thema lassen sich eine Unmenge an Ratgebern und Self-Help-Büchern finden, die sich darauf herunterbrechen lassen, Kontrolle und Achtsamkeit einen exzessiven Medienkonsum entgegenzusetzen: Sie tragen sprechende Titel wie *Digitale Invasion: Wie wir die Kontrolle über unser Leben zurückgewinnen*, *Digitale Erschöpfung: Wie wir die Kontrolle über unser Leben wiedergewinnen*, *Digital Detox: Wie Sie entspannt mit Handy & Co. leben*, *Digital Detox: Der ultimative Leitfaden, um die Technologiesucht zu überwinden, Achtsamkeit zu kultivieren und mehr Kreativität, Inspiration und Ausgeglichenheit in deinem Le-*

8 Pepita Hesselberth, »Detox«, in *Uncertain Archives: Critical Keywords for Big Data*, hg. von Nanna Bonde Thylstrup u.a. (Cambridge, MA: The MIT Press, 2021).

9 »Declutter Your Phone with an App Cleanse«, zugegriffen 14. April 2023, https://datadetoxkit.org/en/privacy/appcleanse/.

10 »Declutter Your Phone with an App Cleanse« [Herv. S.A.].

11 »Befreie Dich von den Standardeinstellungen«, zugegriffen 14. April 2023, https://datadetoxkit.org/de/wellbeing/essentials.

ben zu genießen! und *Das Digital Detox Buch: Das 28-Tage-Programm für ein smartes Leben in digitaler Balance*.[12] Wie Greg Goldberg dies am Begriff des *digital dystopianism* deutlich macht, steckt hinter solchen Ratgebern ein normatives Projekt, in denen verantwortliche Nutzer*innen, die ihren Geräten klare Grenzen setzen, den unverantwortlichen Nutzer*innen gegenübergestellt werden, die sich dem Sog der Technik zu sehr aussetzen und hingeben.[13] Das Analoge geriert dagegen zum Ort der Ruhe, Entspannung und Stille, durch den die eigene Selbstbehauptung und Selbstbestimmung gesichert werden sollen.

Die Ratgeber zu Daten- und digitalem Detox gleichen sich somit darin, so resümiert Hesselberth, dass sie den Nutzer*innen einen bestimmten Umgang mit Technologie vorgeben.[14] Wie mit Begriffen wie Datensparsamkeit schon angedeutet, stellen sie damit eine Aktualisierung von Konzepten der Askese und Diätetik dar, deren wesentliche Wirkungsweise sich in Foucaults *Der Gebrauch der Lüste* nachvollziehen lässt. Darin untersucht Foucault die Problematisierung sexueller Aktivitäten in der klassischen griechischen Kultur des 4. Jahrhunderts v. Chr.[15] Diät tritt in dieser Untersuchung als eine Weise auf, die eigene Existenz zu führen, das heißt, »die Lebensführung mit Regeln auszustatten«[16], sodass »man sich als ein Subjekt konstituiert, das um seinen Körper die rechte, notwendige und ausreichende Sorge trägt«[17]. Schon in der klassischen Variante der Diät findet sich somit ein Anruf an die Verantwortung, die jede*r für den eigenen Körper zu tragen hat. Diese Verantwortung hat sich in der zeitgenössischen Gesellschaft, so zeigt die Rede vom Datendetox, auf die eigenen Daten ausgeweitet. Indem man diese Verantwortung übernimmt und ihr gerecht wird, konstituiert man sich als Subjekt. Im Falle von Datensparsamkeit und -detox bedeutet dies, sich als bewusste Nutzer*in zu konstituieren, die*der sich nicht den Diensten unterwirft, die auf die immer größere Produktion und Extraktion von Daten aus sind, sondern weiß, mit dem eigenen Gerät umzugehen und die unwillkürliche Datenproduktion zu begrenzen. Wie schon

12 Vgl. Archibald D. Hart und Sylvia Hart Frejd, *Digitale Invasion: Wie wir die Kontrolle über unser Leben zurückgewinnen* (Holzgerlingen: SCM Hänssler, 2014); Markus Albers, *Digitale Erschöpfung: Wie wir die Kontrolle über unser Leben wiedergewinnen* (München: Carl Hanser Verlag, 2017); Daniela Otto, *Digital Detox: Wie Sie entspannt mit Handy & Co. leben* (Berlin: Springer, 2016); Alessandro Fiorentini, *Digital Detox: Der ultimative Leitfaden, um die Technologiesucht zu überwinden, Achtsamkeit zu kultivieren und mehr Kreativität, Inspiration und Ausgeglichenheit in deinem Leben zu genießen!* (Independently Published, 2019); Anitra Eggler, *Das Digital Detox Buch: Das 28-Tage-Programm für ein smartes Leben in digitaler Balance* (Wien: Like Publishing, 2019).

13 Vgl. Greg Goldberg, »Antisocial media: Digital dystopianism as a normative project«, *new media & society* 18, Nr. 5 (2016): 785.

14 Vgl. Hesselberth, »Detox«.

15 Vgl. Michel Foucault, *Der Gebrauch der Lüste: Sexualität und Wahrheit 2* (Frankfurt a.M.: Suhrkamp, 1989), 20.

16 Foucault, 131.

17 Foucault, 140.

in der klassischen Variante der Diät, verlangt auch der Datendetox »das Individuum selbst mit einem verständigen Verhalten zu rüsten«[18]. Es braucht »eine reflektierte Praxis«[19], die zwar auf Rat von denen angewiesen ist, die wissen, wie man sich richtig zu verhalten hat, die diesen Rat aber nicht gleich einem Befehl bloß befolgt, sondern aus Überzeugung erwächst. Entsprechend liefert das *Data Detox Kit* sowohl Handlungsanweisungen als auch Erklärungen; es führt Begründungen und Warnungen an, warum es wichtig ist, die eigenen Daten zu schützen. Diese zielen darauf, die Nutzer*innen von der Notwendigkeit eines Datendetox zu überzeugen, um die Nutzer*innen zu veranlassen, so lässt sich erneut mit Foucault anführen, »das geziemende Leben zu führen«[20].

2.2 Souveränität

Der Vergleich zu Diätetik und Askese, wie Foucault sie in *Der Gebrauch der Lüste* beschreibt, drängt sich umso mehr auf, als die Gegenökonomie eng mit der Frage nach Kontrolle und damit nach Souveränität verbunden ist. Wie Foucault aufzeigt, lässt sich die Diät in einen Kontext einordnen, in dem der Fokus auf ein Verhältnis gelegt wurde,

> welches es ermöglicht, daß man sich nicht von den Begierden und Lüsten fortreißen läßt, daß man ihnen gegenüber Herrschaft und Überlegenheit wahrt, […] daß man frei bleibt von jeder inneren Versklavung durch die Leidenschaften und daß man zu einer Seinsweise gelangt, die durch den vollen Genuß seiner selbst oder die vollkommene Souveränität seiner über sich definiert werden kann.[21]

Die Betonung der Unwillkürlichkeit, mit der Daten entstehen und Geräte senden, ohne dass die (unaufgeklärten) Nutzer*innen sich dessen bewusst sind, oder des perfiden Designs, mit dem Nutzer*innen zu immer mehr Konsum angeregt werden, wirft ebenfalls die Frage nach Souveränität auf, die nun allerdings nicht so sehr durch die eigenen Lüste bedroht ist, sondern durch die falschen Dienste und die falsche Nutzung. Über eine Auseinandersetzung mit den sogenannten Cypherpunks lässt sich dieser Bezug zur Frage nach (digitaler) Souveränität im Weiteren explizit machen. Unter der Selbstbezeichnung ›Cypherpunks‹ lassen sich Gruppierungen subsumieren, die sich als Vordenker*innen bzw. Ideengeber*innen für die vorwiegend aktivistisch und aufklärerischen Gruppierungen wie Tactical Tech verstehen lassen. Gemeinsam ist den Cypherpunks insbesondere der aufgeladene Bezug zur

18 Foucault, 140.
19 Foucault, 138.
20 Foucault, 139.
21 Foucault, 43.

Kryptografie und die entsprechenden Technologien als Mittel, mit dem man die eigene Anonymität auf eine Weise schützen kann, die jeder Autorität widersteht, nach dem Grundsatz, dass sich mathematische Probleme mit Macht nicht lösen lassen. Der Begriff ›Cypherpunks‹ bezog sich zu Beginn auf eine kleine Gruppe, die sich 1992 um Eric Hughes, Timothy C. May und John Gilmore (späterer Mitgründer der Electronic Frontier Foundation [EFF], die sich unter anderem für Redefreiheit und Privatsphäre einsetzt) bildete. Der Name übertrug sich dann auf eine Mailingliste, die im gleichen Jahr gegründet wurde.[22] An diese Gründungsgeschichte knüpfen auch heutige Nutzungen des Begriffes an. In dieser Zeit legten sowohl May als auch Hughes zudem jeweils ein Manifest vor: *The Crypto Anarchist Manifesto* (1992) von May und *The Cypherpunk's Manifesto* (1993) von Hughes, die den Bezug von Schutz der Privatsphäre, Anonymität und Souveränität exemplifizieren.

Im dem kurzen *Crypto Anarchist Manifesto* beschreibt May die Möglichkeit, mit den neuen Technologien anonym zu bleiben und das Potenzial, das darin liegt, sich damit dem Staat zu entziehen. Es beginnt mit einer Anlehnung an *Das Kommunistische Manifest* (1848) von Karl Marx und Friedrich Engels, wenn er im ersten Satz proklamiert: »A specter is haunting the modern world, the specter of crypto anarchy.«[23] Der gemeinsame Bezugspunkt zwischen den beiden Manifesten – von May einerseits, von Marx und Engels andererseits – ist dabei nicht der Kommunismus, sondern die Revolution. May imaginiert kryptologische Methoden demnach nicht als Werkzeug einer Reform, das in einem bestehenden staatlichen Gebilde negativen Auswüchsen, etwa Übertritte staatlicher Nachrichtendienste, entgegenwirken kann, sondern als die grundsätzliche Überwerfung bestehender und Gründung neuer Strukturen im digitalen Milieu. Die individuelle Souveränität, mit anderen zu kommunizieren und zu handeln, die durch den Staat und andere Organisationen eingeschränkt wird, wird auf diese Weise befreit: Durch Kryptologie ist es möglich, jedwedem Zugriff Dritter zu entgehen. Diese Techniken seien damit die Drahtschneider zu jenem Stacheldrahtzaun, der erst ermöglicht habe, dass die indigenen Länder im Westen der nordamerikanischen, ehemals britischen Kolonien – der ›Wilde Westen‹ oder »the frontier West«[24] – erschlossen, umzäunt und zu Eigentum gemacht werden konnten. Es werde somit jene Anarchie ermöglicht, die in Westernfilmen imaginiert wird, bevor sich staatliche Strukturen ausbreiteten; sehr deutlich sieht sich May als Cowboy in diesem Szenario, für den dieser Ort

22 Vgl. Robert Manne, »The Cypherpunk Revolutionary: Julian Assange«, *The Monthly*, März 2011, https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary.

23 Timothy C. May, »The Crypto Anarchist Manifesto«, in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, hg. von Peter Ludlow (Cambridge, MA: The MIT Press, [1992] 2001), 61.

24 May, 63.

Freiheit und Möglichkeiten ohne staatliche Regulation bereithält, nicht als Native American.

In dem wenige Jahre später erschienenen Text *Crypto Anarchy and Virtual Communities* (1994), mit dem May eine Erläuterung seines Manifestes liefert, bekräftigt er noch einmal, dass die Anarchie, an die er denkt, nicht eine nicht-hierarchische Form von Kollektivität meint, sich somit nicht an historische Vorbilder wie etwa Michail Bakunin orientiert, sondern eine Anarchie der individuellen Freiheit vom Staat im Sinn hat. Anarchie meint hier, so May, die Abwesenheit der Regierung und sei damit der Anarchie des Anarchokapitalismus ähnlich, »the libertarian free-market ideology that promotes voluntary, uncoerced economic transactions«[25]. Mehr noch als in seinem früheren Manifest, in dem das Umstürzen einer Ordnung im Vordergrund stand – es endete mit dem pathetischen Aufruf »Arise, you have nothing to lose but your barbed wire fences!«[26] – finden sich hier Aspekte, die die Vision einer souveränen Entität unterbreiten. Kryptografie ist nicht mehr der Drahtschneider, sondern »holds up the ›walls‹ of these cyberspatial realities«[27], bietet somit den Schutz, hinter dem sich dann die schon im Manifest imaginierte Freiheit ausbreiten kann. In ähnlicher Weise wird Kryptografie mit Redefreiheit verbunden, zu der gehören solle, dass ein Dialog von den Nachbar*innen oder der Regierung nicht verstanden wird – nicht die ungestrafte öffentliche Rede wird eingefordert, sondern die Möglichkeit uneinsehbarer, geheimer Rede. Dieser zweite Text endet entsprechend mit den nicht weniger pathetischen Worten: »We will be the colonizers of cyberspace.«[28] Damit findet sich hier eine andere Deutung des schon im ersten Text angeführten Siedlungskolonialismus: Cypherpunks treten hier nicht mehr als Cowboys auf, die nach Westamerika vordringen, um eine Freiheit zu finden, die durch den Stacheldrahtzaun begrenzt wird, sondern als Kolonialisierer*innen und damit als diejenigen, die im Raum des Cyberspace Gemeinschaften gründen. Sowohl Westamerika als auch der Cyberspace werden dabei als wesentlich leere Räume imaginiert.

Es ist diese zweite Vorstellung, von Kryptografie als Möglichkeit, souveräne Gemeinschaften zu gründen, die sich auch im *A Cyperpunk's Manifesto* von Hughes wiederfindet. Hughes beschreibt darin Kryptografie als Mittel, Privatsphäre zu schaffen und zu schützen. Privatsphäre meint nicht nur einen privaten im Kontrast zum öffentlichen Raum, sondern allgemein die Möglichkeit, selbst zu entscheiden, wem man wie viel über sich preisgibt. Hughes legt damit die Betonung auf die Kontrolle von Informationen, zu der auch eine Sparsamkeit im Umgang mit Informationen gehört. Wenn aber unwillentlich Informationen offenbart werden, sobald man

25 Timothy C. May, »Crypto Anarchy and Virtual Communities«, in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, hg. von Peter Ludlow (Cambridge, MA: The MIT Press, [1994] 2001), 69.

26 May, »The Crypto Anarchist Manifesto«, 63.

27 May, »Crypto Anarchy and Virtual Communities«, 66.

28 May, 77.

einkauft, jemanden anruft oder eine E-Mail verschickt, dann schränke dies die Privatsphäre ein: »When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself. […] An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.«[29] Cypherpunks sind aufgerufen, eben solche anonymen Systeme zu bauen und zur Verfügung zu stellen. Denn der Schutz von Privatsphäre sei ein kollektives Projekt und verlange einen Gesellschaftsvertrag. Souveränität wird hier als individueller und gemeinschaftlicher Wert ins Spiel gebracht, der im staatlichen Rahmen verloren gegangen ist, aber durch Kryptografie wiedererlangt werden kann.

Diese Überlegungen werden fast 20 Jahre später in einer Diskussion zwischen einigen der wichtigsten Akteure einer Debatte um Datenakkumulationen fortgeführt. Auf Initiative von Julian Assange (vor allem durch WikiLeaks bekannt und selbst Mitwirkender an der Cypherpunk Mailingliste von Hughes, May und Gilmore) haben sich mit ihm noch Jacob Appelbaum (zu dem Zeitpunkt noch unter anderem Entwickler am Tor-Projekt, mit dem man sich anonym im Netz bewegen kann, bevor er 2016 nach Missbrauchsvorwürfen ausgeschlossen wurde[30]), Andy Müller-Maghun (Mitglied und ehemaliger Sprecher des Chaos Computer Clubs) und Jérémie Zimmermann (Mitbegründer und Sprecher von La Quadrature du Net) versammelt. Das Gespräch, zusammen mit einer Einführung von Assange, erschien unter dem Titel *Cypherpunks*. Die Diskussion findet darin unter anderem Vorzeichen statt als bei den früheren Manifesten: Sah gerade May das Internet noch als eine durch den Staat nicht zu kontrollierenden Bereich an, in dem nun eine Freiheit vom Staat möglich sei, beginnt Assange das Diskussionsband folgendermaßen: »This book is not a manifesto. There is not time for that. This book is a warning. […] The internet, our greatest tool for emancipation, has been transformed into the most dangerous facilitator of totalitarianism we have ever seen. The internet is a threat to human civilization.«[31] Die Wandlung vom freien Netz zur größten Bedrohung sei vor allem der durch das Internet ermöglichten Ausweitung der Überwachung geschuldet. Entsprechend werden die Vorläufer von Big-Data-Praktiken in der Diskussion von Assange et al. in der Überwachung einzelner gesucht, etwa wenn Facebook mit der Stasi verglichen und als perfektes Panoptikum bezeichnet wird.[32] Der Unterschied sei nun bloß, dass nicht mehr einzelne Personen als Ziel herausgepickt wer-

29 Eric Hughes, »A Cypherpunk's Manifesto«, in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, hg. von Peter Ludlow (Cambridge, MA: The MIT Press, [1993] 2001), 82.

30 Vgl. Johannes Boie, »Missbrauchsvorwürfe erschüttern Berliner Hacker-Szene«, *Süddeutsche Zeitung*, 6. Juni 2016, https://www.sueddeutsche.de/digital/jacob-appelbaum-missbrauchsvorwuerfe-erschuettern-berliner-hacker-szene-1.3022341.

31 Julian Assange u.a., *Cypherpunks: Freedom and the Future of the Internet* (New York/London: OR Books, 2012), 1.

32 Vgl. Assange u.a., 26.

den würden, sondern es effizienter sei, alles zu sammeln und die Daten im Nachhinein durch analytische Systeme zu durchforsten.[33] Diese Bedrohung, die Ausspähung des gesamten Netzes durch staatliche Geheimdienste wie die NSA oder private Organisationen wie Google, die ihre Daten wiederum Geheimdiensten zur Verfügung stellen (müssen), wurde spätestens mit den Snowden-Enthüllungen 2013 öffentlich bekannt. Auch hier – wie schon bei May und Hughes – taucht also der Staat als wesentlicher Widersacher auf, gegen den man sich nun mit Kryptografie schützen müsse, wodurch man eine ›freie‹, unkontrollierte Sphäre schaffen könne. Wie Assange in der Einleitung in prophetischer Weise proklamiert:

> The universe believes in encryption. It is easier to encrypt information than it is to decrypt it. We saw we could use this strange property to create the laws of a new world. To abstract away our new platonic realm from its base underpinnings of satellites, undersea cables and their controllers. To fortify our space behind a cryptographic veil. To create new lands barred to those who control physical reality, because to follow us into them would require infinite resources. And in this manner to declare independence.[34]

Dieser Ruf nach einer neu zu gründenden Souveränität wird im laufenden Gespräch dann als Kontrolle ausbuchstabiert, die man als Nutzer*in ausüben können muss. Über *Cypherpunks* finden wir nun also den Weg zurück vom Gebot der Souveränität zum Gebot der bewussten Nutzung. Wenn im antiken Griechenland die Sorge umging, dass man von den Lüsten bestimmt wird, weshalb gefordert wurde, stattdessen eine Beziehung der Herrschaft gegenüber den Lüsten aufzubauen, so sind es nun die Maschinen und Algorithmen, die kontrolliert werden müssen, statt von diesen kontrolliert zu werden. Dafür brauche es offene Software, deren Funktionsweise nachvollziehbar ist und Nutzer*innen, die die entsprechenden Kenntnisse haben und den Wert solcher Software erkennen.[35] Es gelte, diese Technologien zu verstehen, das heißt, technologiemündig zu werden, sonst könne man sich wieder nur auf Autoritäten verlassen.[36] Jede*r muss selbst die eigene Privatsphäre schützen (können), um nicht der Alternative, der dystopischen Version zwanghafter Angepasstheit, zu verfallen. Wie es erneut Assange ausdrückt:

> They will either think, »I need to be careful about what I say, I need to conform,« the whole time, in every interaction. Or they will think »I need to master little components of this technology and install things that protect me so I'm able to express my thoughts freely and communicate freely with my friends and people I care about.« If people don't take that second step then we'll have a universal

33 Vgl. Assange u.a., 38f.
34 Assange u.a., 3.
35 Vgl. Assange u.a., 59f.
36 Vgl. Assange u.a., 31f.

> political correctness, because even when people are communicating with their closest friends they will be self-censors and will remove themselves as political actors from the world.[37]

Assange bemüht für die Verantwortung, die Nutzer*innen übernehmen müssen, das alltägliche Händewaschen. Auch dabei hätte es erst eine gewisse Paranoia vor etwas gebraucht, das man nicht sehen kann – die Bakterien, die sich nicht sichtbar auf den Händen befinden und nur durch Seife und Wasser zu entfernen sind –, damit das Händewaschen zu einer Notwendigkeit wurde und die dafür nötigen Technologien wie Seife allgemein verfügbar gemacht wurden. Wie das Händewaschen soll auch die digitale Hygiene zur Gewohnheit werden.

Hackers und damit auch die Gesprächspartner aus *Cypherpunks* werden in dieser Situation von Zimmermann als diejenigen ins Spiel gebracht, die Werkzeuge bauen, um Widerstand zu leisten, und die aufgerufen sind, Nutzer*innen mit ihrem technischen Wissen zu leiten. Sie sind die zeitgenössischen Ärztinnen*Ärzte und Philosoph*innen, die zur richtigen Lebensweise anleiten: »I think it is of tremendous importance that we hackers are here with our technical knowledge to guide people and to tell them, ›You should use this technology that enables control over your privacy rather than Facebook or Google‹.«[38] Wie es schon Foucault in Bezug auf die Diät formuliert hatte, sollen Nutzer*innen nicht bloß einen Befehl folgen, sondern Verantwortung übernehmen, das heißt, mündig werden, und sich gegen die Überwachung durch das Internet wehren. Die Datenaktivist*innen mit den Technologien und dem Wissen, welches sie mitbringen, seien hier, um dabei zu helfen. Sie würden den Weg zeigen, den die Nutzer*innen gehen sollen, sind letztere erst informiert und bereit, bewusst zu handeln.

Hier lassen sich schließlich auch künstlerische Werke anführen, die in ganz ähnlicher Weise Souveränität propagieren. Das Werk mit dem bezeichnenden Namen *Autonomy Cube* (2014) wurde von dem Künstler Trevor Paglen in Zusammenarbeit mit dem bereits erwähnten Appelbaum entwickelt. In der Ausstellung *Global Control and Censorship*, die 2015–2016 im Zentrum für Kunst und Medien (ZKM) stattfand, präsentierte sich das Werk wie die Lösung einer immer wieder beschworenen Bedrohung durch das Netz. Die Arbeit ist auf den ersten Blick sehr minimalistisch: Mehrere Computermainboards sind auf einem weißen Podest hinter dickem Plexiglas installiert. Deren Bedeutung wird erst ersichtlich, wenn sich das eigene Mobilgerät mit dem WLAN-Hotspot des Kubus verbindet. Der *Autonomy Cube* bietet nämlich Zugang zum Tor-Netzwerk. Dieses Netzwerk leitet die Verbindung zur Internetseite, die man aufruft, über verschiedene, zufällige Zwischenstationen, von denen keine gleichzeitig Sender*in und Empfänger*in kennt, sodass der Weg nicht zurück-

37 Assange u.a., 64f.

38 Assange u.a., 69.

verfolgt werden kann. Der *Autonomy Cube* ist eines dieser Relay-Stationen. Die versprochene Autonomie ist somit die Anonymität, die diese Verschlüsselung ermöglicht, die einen Schutz gegen eine umsichgreifende Überwachung darstellt. Durch Kryptografie kapseln sich Nutzer*innen vom allgemeinen, ungeschützten Netz ab; es werden Zwischenstationen als *buffer* eingebaut und durch die Anonymität kontrolliert, wer was von einem sehen kann. Indem Dritte nicht nachverfolgen können, wer die Endnutzer*innen sind oder wo sie sich befinden, wird nur das sichtbar, was man selbst von sich offenbart, statt ungewollt noch zahlreiche weitere Informationen mitzuliefern. Wie in der restlichen Ausstellung wird auch hier das Internet als eine Gefahr angesehen, von der man sich abzugrenzen hat.

Eingerahmt wird diese Arbeit noch dazu auf der einen Seite von Marc Lees *Realtime Stories – mapping the free flow of information around the world in realtime* (2015) und auf der anderen Seite von der Installation *Sehen und gesehen werden* (2015) von Jörn Müller-Quade, Dirk Achenbach, Bernhard Löwe, Jeremias Mechler und Matthias Nagel. *Realtime Stories* ist eine webbasierte Installation, in der Bilder, Töne, Videos und Textnachrichten aus verschiedenen Social-Media-Netzwerken in Echtzeit abgegriffen und projiziert werden. Die immer schon angelegte Öffentlichkeit der Inhalte wird auf diese Weise ausgestellt. *Sehen und gesehen werden* wiederum besteht aus aufeinandergestapelten Bildschirmen, die Bilder von privaten, über unverschlüsselte Webadressen zugänglichen Überwachungskameras abspielen. Man kann somit über die selbst aufgestellten Kameras in die Häuser und Geschäfte der unwissenden Bewohner*innen hineinschauen. Die Botschaft ist: Was online ist, ist in der Regel nicht privat und es ist nicht zu kontrollieren, wer Bilder und Daten anschaut und zu welchen Zwecken benutzt, wenn sie einmal im Netz, das heißt, einmal ›da draußen‹ sind. Man muss sich demnach schützen, so lässt sich aus der in der Ausstellung aufgebauten Drohkulisse schließen, indem man möglichst wenige Daten und Bilder sendet – eine digitale Askese –, die Geräte unter Kontrolle bringt, die ohne das Zutun der Nutzer*innen Daten senden, und die eigene Kommunikation verschlüsselt und sichert.

Auch das Workshopformat *KILLYOURPHONE* (2014) des Künstlers Aram Bartholl legt in dieser Weise eine Lösung vor. Im Workshop werden Handytaschen aus versilbertem Stoff hergestellt, die das Handy oder Smartphone wie einen faradayschen Käfig von allen Signalen abschirmen: Es kann weder empfangen noch etwas gesendet werden. Das Smartphone als ein von sich aus ständig sendendes Gerät wird eingesperrt und damit unter die Kontrolle der Nutzer*innen gebracht. Nur wenn sie es aus der Tasche nehmen, kann es senden, in der Tasche ist es nutzlos, wie tot. Die Nutzer*innen erlangen somit mit Foucault gesprochen das alte, souveräne Recht ihr Gerät »sterben zu *machen* oder leben zu *lassen*«[39].

39 Foucault, *Der Wille zum Wissen: Sexualität und Wahrheit* 1, 134 [Herv. i.O.].

2.3 Kritik der Gegenökonomie

Die Gegenökonomie, so lässt sich nun zusammenfassen, verweist parallel zum Modell der bewussten Konsument*innen auf die Verantwortung der Nutzer*innen: Diese müssten sich bewusst werden, wie schädlich die unwillkürliche Produktion von Daten sowohl für sie selbst als auch für alle anderen Nutzer*innen seien, denn durch diese Daten werde erst eine digitale Ökonomie ermöglicht und erhalten, die auf die Extraktion und Verarbeitung von Daten aufbaut. Um sich dagegen zu wehren, müssten die Nutzer*innen die Kontrolle über ihre Geräte und Dienste und damit letztendlich über ihre Daten gewinnen, statt kontrolliert zu werden und damit Souveränität aufzugeben. Die Gegenökonomie konzentriert sich damit auf die Seite des Konsums der Konsument-Produzent*innen: Indem anders und bewusster konsumiert wird, indem man andere Dienste nutzt oder die Standardeinstellungen anpasst, sollen weniger Daten produziert werden. Man soll aktiv werden, statt sich einer Passivität hinzugeben. Kauft man sich in gewisser Weise die Nutzung der Dienste über die Preisgabe der Daten ein, so soll man nun sparsamer damit umgehen, die Daten enger an sich halten und genau überlegen, bevor man sie veräußert.

Die Gegenökonomie lässt sich nun auf dreierlei Weise kritisieren. Zunächst lässt sich die Kritik wiederholen, die schon zu Beginn des vorherigen Teils mit dem Unterschied von Überwachung und *capture* aufgebracht wurde: Wie bereits dargelegt, ist es wichtig, die Überwachung wie sie etwa durch staatliche Geheimdienste wie der NSA betrieben wird, nicht mit der Logik einer digitalen Ökonomie zu vermischen. Legt man nicht ausreichend dar, worin die Probleme liegen und setzt stattdessen auf die Schockwirkung von Superlativen, können Rezipient*innen schnell zum dem Schluss kommen, dass die derzeitige Situation diesem dystopischen Vergleich nicht standhält, und damit die Kritik an Datenpraktiken insgesamt verwerfen, so Agre 1994.[40] Eine solche Sorgsamkeit in der Kritik und der Unterscheidung verschiedener Datenpraktiken findet sich dagegen selten in der Gegenökonomie, die hofft, ein Gefühl von Bedrohung oder Paranoia werde zu einer bewussteren, datensparsameren Nutzung führen.

Zweitens lässt sich kritisieren, dass die Schuld an dem derzeitigen Modell einer digitalen Ökonomie, das auf der Aggregation und Verarbeitung von Daten aufbaut, laut der Gegenökonomie wesentlich auf den Nutzer*innen zu lasten scheint, trotz der indirekten Position, die diese einnehmen (sie sind nicht die Kund*innen von werbefinanzierten Unternehmen wie Google oder Facebook; wichtig sind nicht die einzelnen Nutzer*innen, solange die Werbeeinnahmen weiterhin fließen). So stoßen auch die Gesprächsteilnehmer von *Cypherpunks* in die Kerbe, demnach die

40 Vgl. Agre, »Surveillance and capture: Two models of privacy«, 116.

Nutzer*innen an der digitalen Misere Schuld sind: Neben der Anrufung der individuellen Verantwortung der Nutzer*innen spricht Zimmermann etwa von Jugendlichen, »sending pictures of themselves drunk or whatever«[41] und verurteilt Appelbaum, dass die Überwachung demokratisiert wurde, das heißt, von allen statt von Einzelnen betrieben wird: »Instead of paying people off the way the Stasi did in East Germany, we reward them [Unternehmen wie Facebook] as a culture – they get laid now. They report on their friends and then, ›Hey, so and so got engaged;‹ ›Oh, so and so broke up;‹ ›Oh, I know who to call now.‹«[42]

Dies lenkt von der Rolle des Systems ab, das erst ermöglicht, Daten zu erfassen, so Hesselberth in Bezug auf Daten- und digitalem Detox: Mit dem Fokus auf Konsum würden die komplexen sozioökonomischen Prozesse ignoriert, in denen Mediennutzung eingebettet ist, und stattdessen die Nutzer*innen als diejenigen eingesetzt, die in Kontrolle sein könnten und damit verantwortlich dafür seien, wie digitale Technologien sie beeinflussen.[43] Gleiches gilt, wenn auf den Sog verwiesen wird, den digitale Technologien qua Design auf Nutzer*innen ausüben. Es sind letztendlich, so unterstreichen die zitierten Ratgeber, die Nutzer*innen, die lernen müssten, sich dem zu entziehen, die lernen müssten, souverän zu sein. Im Gegensatz dazu verweisen Wendy Hui Kyong Chun und Sarah Friedland in *Habits of Leaking: Of Sluts and Network Cards* darauf, dass Netzwerkkarten, über die eine digitale Kommunikation läuft, notwendigerweise offen sein müssen und nicht erst durch eine falsche Nutzung offen werden. Offenheit ist somit im System angelegt.

> A monogamous network card – a network card that only read and wrote your traffic – would be inoperable; if your computers are (retroactively) monogamous, it is because they discretely erase their indiscretions, thus leaving the ordinary user in the dark. […] Your network card is, technically speaking, initially »slutty«: dirty, open to all traffic, indiscriminate (to clean is to delete). Crucially, though, without this necessary vulnerability/openness, there would be no Internet, no communications; our network cards only appear »promiscuous« if we envision our machines as personal.[44]

Chun und Friedland kritisieren, dass die Nutzer*innen als Verursacher*innen von Öffentlichkeit gesehen werden, obwohl diese dem Internet auf Grund der Effekte ihrer technologischen, aber auch sozialen und politischen, Infrastruktur endemisch ist. Sie arbeiten darüber hinaus heraus, wie diese Nutzer*innen, die sich nicht um

41 Assange u.a., *Cypherpunks: Freedom and the Future of the Internet*, 52.

42 Assange u.a., 56.

43 Vgl. Hesselberth, »Detox«.

44 Wendy Hui Kyong Chun und Sarah Friedland, »Habits of Leaking: Of Sluts and Network Cards«, *Differences* 26, Nr. 2 (2015): 5.

ihre Daten scheren, die ›unverantwortlich‹ mit ihren Bildern umgehen, die ihr Handy nicht aus der Hand legen können und die ständig alles posten müssen, die somit aufgeklärt und vor den eigenen Handlungen bewahrt werden müssen, als wesentlich *weiß* und cis-weiblich imaginiert werden. Mit anderen Worten: Gerade anhand der *weißen* cis Nutzer*in* wird die Gefahr, der man sich bewusst werden soll, bzw. die Paranoia, die man notwendigerweise entwickeln soll, exemplifiziert. Was bedroht ist, sind somit auch geschlechtlich markierte und rassifizierte Werte; Werte also, die exklusiv mit Weiblichkeit und *weiß*-sein verbunden sind. Chun und Friedland zeigen auf diese Weise die Parallelen zwischen der Schuld, die den sich exponierenden Nutzer*innen zugeschrieben wird, und der Praxis des *slut-shaming*. *Slut*-shaming meint dabei »the public shaming of women perceived to be promiscuous«[45].

Chun und Friedland führen als erstes Beispiel in der Evidenzkette, die diesen Zusammenhang nachweisen soll, den Fall der damals siebzehnjährigen *weißen* Chelsea Chaney an. 2011 wurde bei einer Veranstaltung über Internetsicherheit an einer Schule ein Foto Chaneys ohne ihre Zustimmung verwendet, welches sie im Bikini neben einem Pappaufsteller des Schwarzen Rappers Snoop Dogg zeigt. In der Präsentation wurde das Foto mit der Unterschrift »›Once It's There, It's There to Stay‹«[46] versehen, suggerierend, dass Chaney sich in und mit dem Foto exponierte und sich dabei unabsehbaren und möglicherweise unliebsamen Konsequenzen in der Zukunft aussetzte. Obwohl das Foto nicht weiter skandalös ist, wird Chaney dafür an den Pranger gestellt, zu freizügig zu sein. Auch die Berichterstattung über einen Fall, der sich 2013 auf einem Eminem-Konzert im Slane Castle, Irland, ereignete, läuft in eine ähnliche Richtung. Auf dem Konzert wurden eine siebzehnjährige Jugendliche und ein Mann bei sexuellen Akten fotografiert. Diese Fotos wurden mit dem Hashtag *#slanegirl* bzw. *#slaneslut* verbreitet. Die Jugendliche kam später ins Krankenhaus, weil sie auf dem gleichem Konzert Opfer eines sexuellen Übergriffs wurde, allerdings nach der fotografierten Szene und nicht durch den im Foto zu sehenden Mann. In der Berichterstattung gibt es nun, wie Chun und Friedland schreiben, eine seltsame Verwirrung und Verwischung zwischen der Zirkulation des Fotos, dem sexuellen Übergriff und der Einlieferung ins Krankenhaus. Mit Titeln wie »›Teenaged Girl Hospitalized after Being Photographed Having Oral Sex‹«[47] stellen diese fälschlicherweise die Verbreitung des Fotos als Grund für ihren Krankenhausaufenthalt dar.[48]

In beiden Beispielen zeigt sich, so Chun und Friedland, dass die Dramatisierung der Gefahr des Web 2.0 nicht mehr primär über die Figur des kleinen Jungen läuft, der pornografischen Inhalten ausgesetzt oder in Chatplattformen von älteren

45 Chun und Friedland, 1.
46 Chun und Friedland, 1.
47 Chun und Friedland, 8.
48 Vgl. Chun und Friedland, 8f.

cis Männern aufgelauert wird, sondern über das junge Mädchen oder die junge cis Frau, welche selbst zum Inhalt wird und pornografisch zirkuliert. Die zirkulierende junge cis Frau stellt somit das Risiko des Internets dar und gilt damit einerseits als selbst schuld, weil sie sich narzisstisch und naiver Weise selbst sichtbar macht, andererseits muss sie ›beschützt‹ werden. Sie ist sowohl *slut* als auch Opfer.[49] Es wird impliziert, dass eine solche Exponierung die cis-weiblichen Subjekte ruiniert, wodurch eine lange, patriarchale Tradition der tugendhaften, bewahrten und zu bewahrenden weiblichen Sexualität wiederholt wird.[50]

> What is significant about the cases of slanegirl, revenge porn victims, and others is that their »ruin« is caused by both their erroneous sexual decision and its online publicity. The traditional idea of female virtue – one that is destroyed by sexual experience or physical exposure – positions ideal female sexuality as contained, private, and invisible. The positioning of slanegirl and others as ruined suggests how the leak – not the sexual act per se – destroys the virtue of its victims. […] This desire to contain female sexuality, to uphold the virtue of virginity, now plays out both in our orifices and our interfaces.[51]

Um der Argumentation von Chun und Friedland zu assistieren, lässt sich ein weiteres Projekt von Tactical Tech anführen. Das inzwischen abgeschlossene, archivierte Projekt *Me and My Shadow* bildete ursprünglich den Rahmen für das *Data Detox Kit* und klärt unter dem Slogan »Take Control of Your Data«[52] sowohl über die Gefahr der digitalen Ökonomie als auch über Lösungswege auf. Ein kurzes Video auf der Homepage stimmte auf das Thema ein. Es eröffnet mit einer grob gezeichneten, farbigen Animation eines Parks mit Menschen, die in der Sonne spazieren und dabei einen Schatten werfen. Ein Rauschen und Flimmern wie auf einem alten Röhrenfernseher verdeutlicht den Wechsel zur digitalen Welt. Man sieht die Welt nun wie durch eine Überwachungskamera gefiltert, in schwarz-weiß mit dem dafür typischen gerahmten Ecken, die den gefilmten Bereich markieren, und einem roten Punkt mit REC für ›Recording‹ daneben. Big-Data-Praktiken werden hier als Überwachung verstanden und entsprechend visuell vermittelt. Das Voiceover bemerkt dazu, dass man nicht nur draußen in der Sonne, sondern auch in der digitalen Welt einen Schatten hat. Diese digitalen Schatten sind im Vergleich zur Einstiegsszene verzerrt, grotesk aufgebläht, langgezogen oder miteinander verschwommen. Sie seien aus Daten zusammengesetzt, so das Voiceover weiter, die sich in der digitalen Umwelt ansammeln. Problematisch seien diese digitalen Schatten vor allem, weil man keine Kontrolle darüber habe, mit was sie sich verbinden, sodass Teile

49 Vgl. Chun und Friedland, 13.
50 Vgl. Chun und Friedland, 9.
51 Chun und Friedland, 9.
52 »Me and My Shadow«, 2016, https://myshadow.org/.

unserer *eigenen* Daten von anderen – Unternehmen und Institutionen – absorbiert werden könnten.[53] Die Animation zeigt dazu Szenen, wie zwei Schatten sich miteinander vereinigen, wie dem Schatten der*des Protagonistin*Protagonisten erst lange Arme wachsen, um einen anderen Schatten zu berühren, und dann Strahlen aussendet, ohne dass dies in der analogen Wirklichkeit auffällt. Die*der Protagonist*in trägt dabei mit Kleid und langen Harren Symbole einer weiblichen Gendernorm. Sie*er setzt den Weg im Park fort und trifft dabei auf einen Hund. Im gleichen Moment transformiert sich der Schatten der*des Protagonistin*Protagonisten. Ihr*sein Schatten wird förmlich durch den Kontakt mit dem Schatten des Hundes infiziert und nimmt eine hundeähnliche Form an. Schließlich läuft die*der Protagonist*in an einem Bürogebäude vorbei und durch den Schatten, den das Gebäude wirft. In dem Moment, in dem sie*er aus dem Schatten heraustritt, greifen Arme wie die Tentakel einer buchstäblichen Datenkrake nach dem Schatten und verleiben sich Teile davon ein. Dass der Schatten außer Kontrolle geraten ist, zeigt sich also daran, dass er unwillkürlich sendet, sich verbindet und verschmilzt. Er ist, in den Worten von Chun und Friedland, zu promiskuitiv, das heißt zu offen. Statt bewussten Kontakt zu bestimmten Nutzer*innen zu suchen, verbindet er sich wahllos mit all den anderen Schatten im Park, gleich ob diese von Menschen, Tieren oder Gebäuden geworfen werden. Zwar wird mit Letzterem auch eine gewisse Gewaltförmigkeit dargestellt – Teile des Schattens werden von dem Gebäudeschatten förmlich weggerissen. Größtenteils ist es aber doch der von der*dem als weiblich markierten Protagonistin*Protagonisten geworfene Schatten selbst, der bereitwillig Verbindungen sucht und sich den Interaktionen mit anderen öffnet.

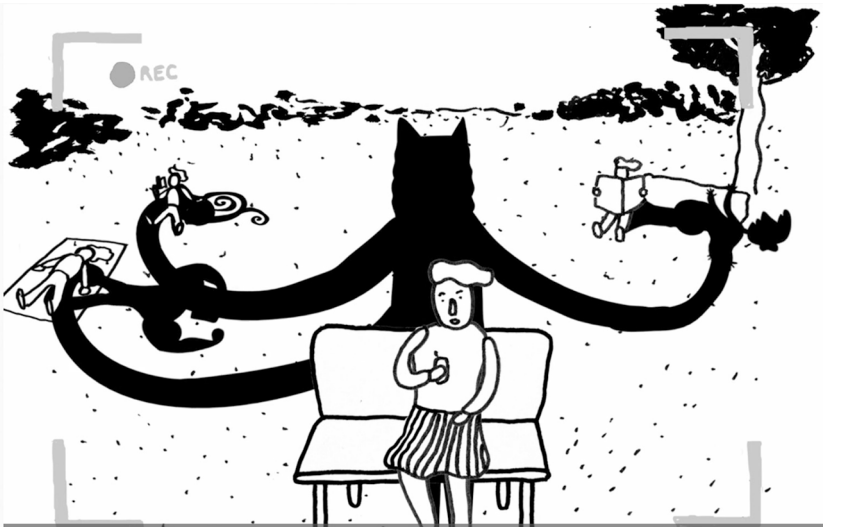
Damit setzt sich hier nach Chun und Friedland ein Schutz von *weißer* Weiblichkeit fort, der schon das Aufkommen der US-amerikanischen Gesetze zum Schutz von *privacy* Anfang des 20. Jahrhundert motivierte, wie unter anderem Eden Osucha in *The Whiteness of Privacy* argumentiert. *Privacy* lässt sich dabei mit Privatsphäre übersetzen, umfasst aber in der Argumentation auch das Recht am eigenen Bild. Demnach konstituierte sich ein Recht auf Privatsphäre durch den 1890 erschienenen, in *Harvard Law Review* veröffentlichten Artikel *The Right to Privacy* von Samuel Warren und Louis Brandeis und den darauf im Wesentlichen aufbauenden Fall *Roberson v. Rochester Folding Box Company* von 1902. Beide waren entscheidend, um schließlich 1903 ein erstes Gesetz zum Schutz der Privatsphäre im Bundesstaat New York einzuführen.[54] Der Artikel reagierte auf eine Zunahme von Bildern und deren Zirkulation in Presse und auf Produkten, die durch die Rollfilmkamera, die 1888 auf den US-Markt kam, ermöglicht wurde. Man saß nun nicht mehr für ein Porträt, so Warren und Brandeis, sondern ein Bild wurde (auf-)genommen, ohne dass man als

53 Vgl. »Me and My Shadow« (Video, 1 min 37 sec, 2016), https://myshadow.org/.

54 Vgl. Eden Osucha, »The Whiteness of Privacy: Race, Media, Law«, *Camera Obscura* 24, Nr. 70 (2009): 67ff.

›verletzte‹ Partei an dieser Aufnahme aktiv teilnehmen musste.[55] Der Blick der medialen Öffentlichkeit wurde dabei als intrinsisch pornografisch beschrieben, auch hier ist dabei das prädestinierte Opfer einer imaginierten Exponierung weiblich. So wie Porträts schon immer zwischen einer bürgerlich-repräsentativen und einer kriminalisierend-repressiven Funktion schwankten, impliziert die von Warren und Brandeis beschriebene mediale Umwelt nun, dass auch bürgerliche Porträts das kulturelle Ideal des Selbstbesitzes [»self-ownership«[56]] durch ihre Zirkulation destabilisieren können.[57]

Abb. 1: Screen Capture (Tactical Tech – Me and My Shadow [2016])



Der Fall *Roberson v. Rochester* schloss an diese Argumentation an. Abigail Roberson klagte dagegen, dass ihr Bildnis von der Rochester Folding Box Company benutzt wurde. Die Firma hatte ein Bild von ihr im Profil von einem Fotografen gekauft, um eine Mehlmischung zu bewerben. Wie bei Warren und Brandeis wurde auch in diesem Fall argumentiert, dass die Verletzung durch die unrechtmäßige Verwendung eines Bildes tiefer gehe als bei einem bloßen Vertragsbruch oder Diebstahls. Denn indem dieses Bild in öffentlichen Orten zirkulierte, die Roberson selbst nie aufgesucht hätte, so die Anklage ihrer Anwälte, ist ihr die gleiche Scham

55 Vgl. Osucha, 85.
56 Osucha, 76.
57 Vgl. Osucha, 76.

und das gleiche Leid aufgeladen worden, als sei sie selbst verkauft und an diese Orte gebracht worden. Es ging nicht darum, dass falsche oder unvorteilhafte Gerüchte oder Darstellungen kursierten, somit ihr sozialer Ruf in Verruf gerate. Es ging somit nicht um die Weise *wie* sie von anderen wahrgenommen wurde – tatsächlich wurde das Bild als ›schmeichelhaft‹ beschrieben –, sondern es ist die bloße Existenz und Zirkulation eines Bildes, *dass* sie also überhaupt an bestimmten Orten außerhalb ihrer üblichen Umgebung wahrgenommen werden kann, die den Schaden ausmacht.[58] Die Verletzung ihrer Privatsphäre und ihres Rechts am eigenen Bild lieferte dabei gleichzeitig die Evidenz, dass ein solches zu schützendes Recht überhaupt existiert.[59]

Es ist nach Osucha kein Zufall, dass sich das Recht am eigenen Bild und auf Privatsphäre gerade durch einen Fall etablierte, der die Verletzung einer *weißen* Frau verhandelte. Einerseits sind, wie Eva Cherniavsky beobachtet, *weiße* cis Frauen »required to embody interiority *for others*«[60]. Andererseits sei die Öffentlichkeit aber auch auf eine bestimmte Weise als eine Sphäre der Enteignung etabliert, die diese gerade für *weiße* cis Frauen als Übertretung erscheinen lässt. Osucha argumentiert, dass der mediale Blick gerade deswegen als intrinsisch pornografisch und die Verbreitung des Bildes gerade deswegen als enteignende Kommodifizierung wahrgenommen wurde, weil die mediale, US-amerikanische Öffentlichkeit bereits durch die Darstellungen von rassifizierten Körpern und rassistischen Ikonografien geprägt war. Diese Prägung zog sich durch die öffentliche Examinierung auf dem Sklavenblock,[61] zum *weiß*-männlichen Blick wissenschaftlicher Untersuchungen bis zu Ministrel Shows, in denen *weiße* Darsteller*innen in Blackface stereotypisierte Schwarze Menschen darstellten. Diese Stereotypen fanden sich schließlich auf Produkten wieder, wenn etwa die ›mammy figure‹ auf Haushaltswaren abgedruckt wurde und damit die Fantasie einer Schwarzen Unterwürfigkeit perpetuierte.[62] Auch wenn bei Letzterem gemalte Bilder von nicht notwendigerweise real existierenden Personen statt Fotos abgebildet wurden, rechnet Osucha diesen Darstellungen einen entscheidenden Einfluss an der Konstituierung der Öffentlichkeit als enteignende Sphäre zu.[63] Die Zirkulation des Bildes einer *weißen* Frau wurde somit als enteignend gesehen, weil sie dadurch in die Nähe derjenigen rassifizierten und (ehemals) versklavten Körpern gerückt wurde, die man bereits in der Öffentlichkeit, in Shows und auf Produkten sah. Das Recht auf Privatsphäre

58 Vgl. Osucha, 84.

59 Vgl. Osucha, 95f.

60 Eva Cherniavsky, *Incorporations: Race, Nation, and the Body Politics of Capital* (Minneapolis, MN: University of Minnesota Press, 2006), xxv [Herv. i.O.].

61 Vgl. Osucha, »The Whiteness of Privacy: Race, Media, Law«, 79.

62 Vgl. Osucha, 80f.

63 Vgl. Osucha, 82.

sollte somit nach Osucha auch der Stabilisierung von ethnischen Grenzen in einer Zeit nominaler Gleichheit dienen.[64]

Die *Weißheit* der Privatsphäre zeigt sich dabei im Vergleich zu Reaktionen auf die Darstellung Schwarzer Frauen zur gleichen Zeit. Denn während die Zirkulation von Roberson problematisiert wurde, schien die Zirkulation und Kommodifizierung von Nancy Green, einer ehemals versklavten, Schwarzen Frau, unkritisch zu sein. Green wurde engagiert, um die stereotype Figur ›Aunt Jemima‹ auf Messen und Veranstaltungen darzustellen. Die Figur wurde 1890 – also etwa zum Zeitpunkt der Veröffentlichung von *The Right to Privacy* und der Verhandlung von *Roberson v. Rochester* – als das Logo für einen Pfannkuchenmix eingeführt. Erst nach den Black Lives Matter-Protesten 2020 kündigte Quaker Oats, das die Rechte an der Marke inzwischen hält, an, dass der Name und das entsprechende Bild abgesetzt werden würden.[65] In den Anfängen der Marke wurde Green als die ›originale‹ Aunt Jemima angekündigt; es existierte darüber hinaus eine Biografie der fiktionalen, auf einer Blackface-Darstellung basierenden Figur und Green war mit einem Vertrag auf Lebenszeit an das Copyright der Figur gebunden. Auf diese buchstäbliche Kommodifizierung, bei der aus Green eine mediale Figur gemacht wurde, die darauf angelegt war, sich zu verkaufen, gab es allerdings keinen Aufschrei. Osucha resümiert:

> That, in the same historical moment, the literal commodification of one woman – African American, elderly, working class – would be enthusiastically embraced by American consumers, while another – white, young, bourgeois – woman's rather tenuous, purely symbolic claim of commodification was met with proportionate horror and condemnation helps highlight […] the specific racial, gendered, and class contours of the injuries claimed by Abigail Roberson and of the legal doctrine that this seminal lawsuit engendered.[66]

Wie unterschiedlich die beiden Fälle gehandhabt wurden, zeigt somit, wem ein Recht und ein Besitz am eigenen Selbst zugeschrieben wurde, und wessen Anspruch darauf schon immer prekär war.[67] Indem die Gegenökonomie somit ähnlich wie die NSA und andere Geheimdienste die Leaks und die Übertretung von Grenzen anprangert, wiederholen sie gleichzeitig von Sexismus und Rassismus geprägte Kategorien und Wertvorstellungen. Statt den Nutzer*innen die Schuld zuzuschieben, zu offen in einem Milieu zu sein, welches bereits auf technischer Ebene offen sein muss, das heißt, sich verbinden muss, um überhaupt zu funktionieren, verteidigen

64 Vgl. Osucha, 98.

65 Vgl. Ben Kesslen, »Aunt Jemima brand to change name, remove image that Quaker says is ›based on a racial stereotype‹«, *NBC News*, 17. Juni 2020, https://www.nbcnews.com/news/us-news/aunt-jemima-brand-will-change-name-remove-image-quaker-says-n1231260.

66 Osucha, »The Whiteness of Privacy: Race, Media, Law«, 87.

67 Vgl. Osucha, 79.

Chun und Friedland deshalb das Recht auf Zugang zu öffentlichen Orten und das Recht offen und öffentlich zu sein. Sie bringen dazu den Text *Why Loiter? Women and Risk on Mumbai Streets* von Shilpa Phadke, Sameera Khan und Shilpa Ranade in die Diskussion. In dem Text wird beschrieben, wie ein Diskurs um Sicherheit schnell zu Protektionismus führt und somit den Effekt hat, cis Frauen aus öffentlichen Orten zu vertreiben und als ›gefährlich‹ wahrgenommene cis Männer – vorwiegend Muslime – einer erhöhten polizeilichen Kontrolle zu unterwerfen.[68] Die Autor*innen schlagen deshalb vor, für ein Recht auf Herumlungern [»the right to loiter«[69]] zu kämpfen, das gleichzeitig ein Recht auf Vergnügen und ein Lackmustest für das Recht auf Öffentlichkeit sei.[70] Chun und Friedland nehmen diesen Vorschlag auf und fragen sich, was ›herumlungern‹ im Internet bedeuten könnte und wie das digitale Milieu als öffentlicher Ort gedacht werden kann. Sie kommen zum folgenden Schluss:

> We need to engage in a politics of forgiveness and deletion in which we remember that to delete is not to forget, but to open other less inflexible ways of remembering. To forgive is to give in excess, to give away: to create give in the system by giving way, by giving more than what one gets. That is, to build an Internet that embraces its status as a public domain, in which there is no »promiscuous« mode because there is no monogamous mode, we need to inhabit things differently: to develop new habits of connecting that disrupt the reduction of our interactions to network diagrams that can be tracked and traced. […] Most important, we need to create ways of occupying networks that thrive in the shadowy space between identity and anonymity, that thrive through repetition.[71]

Es ist in diesem Geiste, der in der Wiederholung gedeiht und der nach neuen Wegen sucht, sich zu verbinden, Netzwerke zu besetzen und im Exzess zu geben, in dem ich auch die folgenden Überlegungen zur digitalen Desökonomie verorte. Denn wie Chun und Friedland gezeigt haben, ist die Gegenökonomie vielleicht eine Option für die *weißen* Männer des Cypherpunks, die sich als die neuen Gründerväter eines hinter der Kryptografie geschützten, souveränen Ortes imaginieren.[72] Wie mit dem Verweis auf *Disidentifications* von Muñoz aber bereits betont wurde, sind es insbesondere marginalisierte Subjekte, die sich auf die Binarität von Sicherheit einerseits, Offenheit andererseits nicht einlassen können, wenn Sicherheit gleichzeitig

68 Vgl. Shilpa Phadke, Sameera Khan und Shilpa Ranade, *Why Loiter? Women and Risk on Mumbai Streets* (New Delhi: Penguin, 2011).

69 Phadke, Shilpa, Sameera Khan und Shilpa Ranade »Why loiter? Radical possibilities for gendered dissent«, in *Dissent and Cultural Resistance in Asia's Cities*, hg. von Melissa Butcher und Selvaraj Velayutham (London/New York: Routledge, 2009), 198.

70 Vgl. Phadke, Ranade und Khan, 186 und 198.

71 Chun und Friedland, 19f.

72 Vgl. Assange u.a., *Cypherpunks: Freedom and the Future of the Internet*, 3.

mit einem verminderten Zugang und verminderten Expressionen einhergeht. Sie brauchen, wie Chun und Friedland dies formulieren, andere, neue Wege, sich zu vernetzen.

Der Verweis auf *Disidentifications* führt zudem zum dritten Kritikpunkt an der Gegenökonomie. Neben der Verlagerung der Schuld auf die Schultern der Nutzer*innen, misslingt in der Gegenökonomie auch, die wesentliche Prämisse der digitalen Ökonomie in Frage zu stellen: Das Daten stets eine Ressource darstellen und somit mehr Daten einen größeren Ressourcenreichtum versprechen. Indem die Gegenökonomie darauf abzielt, über den Konsum die Produktion von Daten zu unterbinden, indem sie Detox und Sparsamkeit verschreibt, bekräftigt sie noch den Wert, der von Daten ausgeht und nun in den Händen von Unternehmen wie Facebook oder Google liegt. Ein Dialog aus *Cypherpunks* zwischen Jérémie Zimmermann und Andy Müller-Maguhn, in dem sie die gängige Vorstellung aufgreifen, dass Dienste wie Google oder Facebook einen besser kennen als man sich selbst, liest sich dann als beste Werbung für Google.

> JÉRÉMIE: […] If you're a standard Google user Google knows who you're communicating with, who you know, what you're researching, potentially your sexual orientation, and your religious and philosophical beliefs.
> ANDY: It knows more about you than you know yourself.
> JÉRÉMIE: More than your mother and maybe more than yourself. Google knows when you're online and when you're not.
> ANDY: Do you know what you looked for two years, three days and four hours ago? You don't know; Google knows.[73]

Kritisieren sie hier noch Google oder preisen sie nicht vielmehr dessen enorme Fähigkeiten an, auf die es die Werbekund*innen von Google schließlich abgesehen haben? Wie es in der Definition von Identifikation und Gegen-Identifikation schon angelegt ist, lässt sich somit schließen, dass auch die Gegenökonomie die Annahmen der Ökonomie reproduziert. Dies ist nicht weiter verwunderlich, wenn man bedenkt, wie Hesselberth betont, dass es vielfach (ehemalige) Silicon-Valley-Designer*innen und -Ingenieur*innen sind, die die Aufklärung über die »*informational dominance* in the mass aggregation of data«[74] betreiben. Und auch Zuboff gibt zu Protokoll, dass ihre Analyse wesentlich auf Interviews mit Datenwissenschaftler*innen aus dem Silicon Valley basieren: »In addition, between 2012 and 2015 I interviewed 52 data scientists from 19 different companies with a combined 586 years of experience in high-technology corporations and startups, primarily in Silicon Val-

73 Assange u.a., 51.

74 Hesselberth, »Detox« [Herv. i.O.].

ley.«[75] Es sind somit dieselben oder zumindest ähnlich sozialisierte Personen, die die Systeme einer digitalen Ökonomie gebaut haben und nun vor deren Konsequenzen warnen. Etwas verallgemeinernd könnte man also sagen, dass von Erbauer*innen und Programmierer*innen solcher Technologien deren Wirkungskraft unterstrichen als auch andere Technologien als Lösung und Schutz ins Spiel gebracht wird.[76] Es ist damit nicht überraschend, dass sich Problem und Lösung in vielem gleichen und der Blick für andere Wege, wie ich sie hier unter dem Begriff einer Desökonomie versammeln werde, verschlossen bleibt. Erst die digitale Desökonomie erlaubt dann, die Annahme zur Wertigkeit von immer mehr Daten in Frage zu stellen. Ich folge deswegen im Weiteren nicht ›Expert*innen‹, sondern versuche mich über die verschiedenen Künstler*innen, deren Arbeiten ich besprechen werde, jenen Nutzer*innen zu nähren, die in der Gegenökonomie als zu offen und zu wenig bewusst handelnd beschrieben werden. Ich will zeigen, wie sich auch hier, in der Nicht-Souveränität, ein kritisches Verhältnis vorfinden lässt, welches sich aber nicht durch eine ablehnende, sondern ambivalente Beziehung zur digitalen Ökonomie auszeichnet und sich dabei auf die Produktions- statt die Konsumebene bezieht.

75 Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Kap. 1 – Home or Exile in the Digital Future (VI. The Outline, Themes, and Sources of this Book).

76 Vgl. Hesselberth, »Detox«.