Humboldt-Universität zu Berlin
Mathematisch-Naturwissenschaftliche Fakultät
Institut für Informatik

GNUnet und Informationsmacht: Analyse einer P2P-Technologie und ihrer sozialen Wirkung

Diplomarbeit

zur Erlangung des akademischen Grades
Diplominformatiker

eingereicht von: Christian Ricardo Kühne

Gutachter/innen: Prof. Dr. Wolfgang Coy
Dr. Constanze Kurz

eingereicht am: 16.4.2015 (aktualisiert am 19.03.2016)

Vorbemerkung

Das schriftstellerische Handwerk ist der Informatik des Öfteren absonderlich und wo sie aufgeboten wird, beschaut man sie mit dem kühlen Blick einer technischen Wissenschaft. Wer die Welt nun aber zu deuten gelernt hat, mag darin einen gewissen Wert für sich entdecken. Es bedarf allerdings gewisser sozialer Freiheiten, um dieser Tätigkeit den nötigen Raum zu verschaffen, und ich verdanke diese Freiheiten vor allem meinen Eltern, meiner lieben Carol und Wolfgang Coy. Letzterer hat auch für ein besonderes geistiges Umfeld kritischer DenkerInnen gesorgt, so dass ich auch Andrea Knaut, Stefan Ullrich, Jörg Pohle und meinem guten Freund Rainer Rehak zu danken habe. Ich danke auch Christian Grothoff für die Revision der technischen Aspekte.

Die vorliegende Arbeit stellt eine überarbeitete Fassung meiner Abschlussarbeit dar, die ich im Jahr 2015 an der Humboldt-Universität zu Berlin am Lehrstuhl für Informatik in Bildung und Gesellschaft eingereicht habe. Sie enthält einige substantiellen Änderungen, die vor allem den Abschnitt zur Folgenabschätzung des GNUnets und den Abschnitt mit dem Vorschlag zur Einordnung und Bewertung des GNUnet betreffen.

Zusammenfassung

Diese Arbeit setzt sich mit den Ideen und der Geschichte des GNUnet-Projektes und dem GNUnet als Peer-to-Peer-Netzwerktechnologie auseinander. Es untersucht insbesondere die emanzipatorischen Potentiale im Hinblick auf Formen informationeller Macht und versucht die wesentlichen Machtverschiebungen als Folgenabschätzung eines breiten Einsatzes zu identifizieren: (a) die Machtverschiebung im Bereich der Informationsverarbeitung und (b) die Machtverschiebung im Bereich der Kommunikationsverarbeitung. Zudem wird eine Brücke zum kritischen Datenschutzprojekt geschlagen, um mit ihrer umfassenden gesellschaftstheoretischen Sichtweise das Verhältnis von GNUnet und dem Problem der Informationsmacht schärfer zu bestimmen. Nicht zuletzt wird auch das konstruktive Zusammenspiel dieser beiden Projekte als erforderliches Ziel weiter ausbuchstabiert.

Abstract

This thesis studies the GNUnet project comprising its history, ideas and the P2P network technology. It specifically investigates the question of emancipatory potentials with regard to forms of information power due to a widely deployed new Internet technology and tries to identify essential suspensions of power within the scope of an impact assessment. Moreover, we will see by contrasting the GNUnet project with the critical data protection project, founded on social theory, that both are heavily concerned about the problem of illegitimate and unrestrained information power, giving us additional insights for the assessment. Last but least I'll try to present a scheme of how both approaches may interact to realize their goals.

Inhaltsverzeichnis

Teil I.
Einleitung

»Es ist meist unmöglich, ein überkomplexes Problem einfach zu ›lösen‹, eben weil man seine Problemstruktur noch gar nicht beherrscht – und fast alle sozialen Probleme sind überkomplex. [...] Häufig weiß man erst am Ende der Arbeit, wo das Problem ›in Wirklichkeit‹ liegt! Bei diesen bösartigen Problemen muss man, klüger geworden, immer wieder anfangen – für ›Angewandte‹ ein vertrautes Problem.« – Wilhelm Steinmüller

1. Problemaufriss

Die aufgekommene Machtproblematik im »Informationsbereich« im Zuge der informationstechnologischen Revolution[1] und die davon betroffenen Freiheiten in modernen Gesellschaften zu Beginn der Turing-Galaxis[2] sind der Ausgangspunkt dieser Arbeit. Trotz der denkbar positiven Möglichkeiten, welche die Informationstechnologien in Aussicht stellten, haben wir es bis dato mit einem Bündel negativer historischer Tendenzen zu tun, von denen zwei hier von besonderen Interesse sind: die Auswüchse autoritärer und flächendeckender Überwachungs- und Kontrollsysteme einerseits, und andererseits die hypertrophe Verdatung von Individuen und Gesellschaft mit der Einführung rechnergestützter Informationssysteme in alle gesellschaftlichen Bereiche. Zwar gibt es nützliche Verdatung, ohne die eine moderne Gesellschaft im Grunde genommen nicht existieren könnte,[3] aber die bittere Erfahrung im Umgang mit Informationssystemen als Risikotechnologie ist, dass Grundrechte verletzt werden und demokratischen Institutionen verfallen oder »erodieren« und letztlich Menschen darunter leiden.

Die konkreten negativen Auswirkungen ungebändigter Informationsmacht, die in dieser Arbeit noch genauer spezifiziert wird, sind vielfältig: angefangen bei subtilen Formen wie der Manipulation ökonomischer Präferenzen oder künstlicher Bedürfnisgenerierung durch verführerische Werbung, die Manipulation »digitaler Öffentlichkeit«, Wirtschaftsspionage, die Hintergehung politischer Institutionen wie dem G20-Gipfel oder der UN-Klimakonferenz in Kopenhagen bis hin zu mörderischen Härtefällen von Drohneneinsätzen.[4]

[1] Soziologisch knüpfe ich hier an den Ergebnissen von Castells (2004, S. 31 ff.) an, welcher wiederum den historischen Begriff einer technologischen Revolution vom Typ »informationstechnologisch organisierter kultureller Transformationen« zum Ausgangspunkt nimmt. Das impliziert zumindest, dass sie keine bewußt betriebene, nach emanzipatorischen Zielen ausgerichtete, und daher – man möchte sagen – Menschen gemachte Revolution ist.

[2] Dazu die Kulturanalyse von Coy (1996) unter den epochalen Bedingungen digitaler Medien und mit einer schärferen Aufschlüsselung der betroffenen kulturellen Sphären hinsichtlich der informatischen Wirkungen.

[3] Nach Steinmüller (1993, S. 467).

[4] Zu den Auswirkungen der Bedürfniskontrolle siehe Kurz und Rieger (2010). Zu den Auswirkungen auf die Öffentlichkeit siehe Greenwald (2014). Beispielhaft für die politischen und wirtschaftlichen Auswirkungen siehe MacAskill et al. (2013) und Vidal und Goldenberg (2014). Drohneneinsätze auf Basis von Metadaten sind bei Scahill und Greenwald (2014), Eudes und

Allgemein gibt es verschiedene (sogar gleichzeitig begehbare) Wege in modernen Gesellschaften, um das technikinduzierte Problem unkontrollierter und nicht legitimierter Informationsmacht zu behandeln, die Grundrechte zu wahren und die Erosion der Institutionen zu vermeiden: Rechtstaatlichkeit, wirtschaftliche Anreizsysteme, Technikgestaltung oder auch Bildung (als der mitunter entbehrungsreichste und unberechenbarste Weg) sind hierzu angetan. Auf dem Weg der Technikgestaltung mit wissenschaftlichen Anspruch, versucht es das GNUnet-Projekt seit 2001, dessen Ziel die Erforschung von Möglichkeiten und Grenzen von sicherer Peer-to-Peer-Kommunikation ist. Versuchen wir einen Blick auf die konkreten Ideen und Modelle, um meinem Vorhaben Greifbares zu geben.

1.1. Der Gegenstand

Inhaltlich tritt das Projekt gegenüber anderen Ansätzen von sicheren Kommunikationssystemen durch seine Radikalität hervor, indem es die heutigen Probleme der technologischen Basis unserer Informationsgesellschaft als Folge alter und unbedarfter Entwurfsentscheidungen sowie der dramatischen historischen Entwicklung auffasst und aus dem Wissen um ihre Fehler und Schwachstellen eine neue Architektur nach dem Clean-Slate-Ansatz verfolgt. Das Projekt ist ein prototypisches Beispiel für eine technische Fundamentalkritik und lässt sich durch und durch als einen praktisch umgesetzten Widerstand gegen das »schon immer Dagewesene« lesen und deuten.

Im Kern handelt es sich dabei um einen erweiterbaren Netzwerk-Stack, der alle wichtigen Netzwerkdienste für eine sichere, dezentrale, hierarchielose und teilweise anonym organisierte globale Kommunikation und Datenverarbeitung zur Verfügung stellen soll. Der Peer-to-Peer-Ansatz reflektiert und vermeidet die Kompromittierbarkeit zentralisierter und hierarchisch organisierter Netzwerkdienste wie zum Beispiel die IP-Adressvergabe durch die IANA, dem Domain Name System (DNS) einschließlich DNSsec oder der aktuell eingesetzten Public Key Infrastructure (PKI) für Ende-zu-Ende-Verschlüsselung, bestehend aus X.509-CA und X.509-

Grothoff (2015) und mit erschreckender Auführlichkeit in den »Drone Papers« von The Intercept beschrieben.

Zertifikaten. Neue Algorithmen für die Link-Verschlüsselung, verteiltes Routing und Ende-zu-Ende verschlüsselter Transport lassen die alten unsicheren Protokolle hinter sich, darunter ARP (Spoofing), DHCP (Spoofing, Ressource Exhaustion), IP/BGP (Verletzbarkeit der Netzneutralität) und TCP/UDP (fehlende Authentisierung und Verschlüsselung, RST-Angriffe).[5] Dabei entgegnet das GNUnet dem Vorwurf der unerreichbaren Utopie durch den Ansatz des Netzwerk-Overlaying, das eine »weiche« Transition vom Internet, wie wir es kennen, hin zum GNUnet ermöglichen soll. Den letzten Stein der Kritik bildet die Eingliederung in das GNU-Projekt, das sich den vier fundamentalen Freiheiten für den Umgang mit Software verschrieben hat: »Die Freiheit, (0) das Programm auszuführen, (1) das Programm in Form von Quellcode zu untersuchen und zu ändern, (2) exakte Kopien weiterzuverbreiten und (3) modifizierte Varianten zu verbreiten«.[6] Eine Konsequenz dessen ist die Herstellung von Bedingungen, unter denen die Kontrolle über die Algorithmen und den Rechenprozess selbst wiedererlangt werden kann und damit letzten Endes – so der Wunsch – auch die Kontrolle über das eigene Leben. Wenn ich mit dem GNUnet die Verwirklichung emanzipatorischer Ziele derartig verbinde, dann erschließt sich logisch auch der zugehörige Objektbereich, nämlich die Gesellschaft, ihre informationstechnologische Basis und die ihr innewohnenden Machtstrukturen.

Das GNUnet wird aus der (Kern-)Informatik heraus erforscht und entwickelt und bildet auch den Gegenstand dieser Arbeit.

Nun wirft bei all dem Gesagten dieser Versuch auf technischem Wege beim näher Hinsehen die Frage auf, wie eigentlich die komplexe, aus den Fugen geratene Informationsmacht verändert werden soll, wie also der Sprung von einer ethisch motivierten Problemsicht zur Technik vonstatten geht und schließlich in einem weiteren Sprung die soziale Realität zu ändern vermag. Interessanter noch ist die Frage, welche Theorien des Sozialen überhaupt der Technikgestaltung zugrunde gelegt werden. In seinem Vortrag »Tools for Breaking out of PRISM«[7] (2014) stellt Christian Grothoff als Leiter des GNUnet-Projekts die rhetorische Frage: »Can we develop technologies to solve problems created by technology?«. Das stimmt

[5] Vergleiche Grothoff et al. (2014, S. 2).
[6] Im Internet: https://gnu.org/philosophy/free-sw, Stand: 6.3.2015.
[7] Im Internet: https://www.youtube.com/watch?v=1lcauMH70cA, Stand: 16.12.14.

skeptisch. Dabei lässt sich aus der Geistes- und Kulturgeschichte heraus ein so grob daherkommendes Unterfangen scheinbar leicht eines kruden Technizismus bezichtigen. Hallt hier nicht die alte Losung der »Cyber-Utopians« nach, die in den 1990er die befreienden Potentiale des Internets proklamierten? Wenn der Politikwissenschaftler Evgeny Morozov schreibt,

> »failing to anticipate how authoritarian governments would respond to the Internet, cyber-utopians did not predict how useful it would prove for propaganda purposes, how masterfully dictators would learn to use it for surveillance, and how sophisticated modern systems of Internet censorship would become«,[8]

ist dies nur die erste Demarkationslinie. Eine weitere stellt sich ein, wenn Gesellschaft und Technik in Wechselwirkung stehen und selbst bei bestehenden Alternativen – man denke an Facebook und Diaspora – ein Wechsel sich als schwierig erweist.

Demgegenüber lasse ich mich hier von einer anderen Vermutung leiten, nämlich dass die »konstruktive Ursachen- und Folgen-Veränderung« (Steinmüller) bei der Technikgestaltung neue politische Spielräume schafft.

1.2. GNUnet und Gesellschaft

Problemstellung

Aus Sicht der Disziplin Informatik und Gesellschaft stellt sich das Problem, wie der Weg des GNUnet-Projektes (samt seiner technischen Komplexität!) einzuordnen und unter den realen gesellschaftlichen Bedingungen zu bewerten ist. Man muss davon ausgehen, dass »reale Aufgaben der Informatik im Kontext [entstehen], im Kontext geformt [werden] und von ihrem Kontext [abhängen]«.[9] Ansonsten ist eine Verkehrung von Zwecken und Mitteln erwartbar. Den Kontext bilden die politischen, rechtlichen, ökonomischen, sozialen und kulturellen Rahmenbedingungen. Dabei geht es nicht darum, alle Aspekte gleichermaßen abzudecken, sondern die gesellschaftsrelevanten Aspekte zu entwickeln und daraufhin die Möglichkeiten und Grenzen einer Technologie herauszupräparieren. Für die Wissenschaft hat die-

[8] Morozov (2012, S. xiv).
[9] Coy (2004, S. 482).

ses Problem in einer Zeit rasanter technischer Entwicklungen an Aktualität nichts verloren – man möchte meinen, sogar an Bedeutung gewonnen. Die Schwierigkeit für die Informatik im Bezug auf ihre Anwendungen liegt so dann darin, Schnittstellen für weitere gesellschaftliche Diskurse bereitzustellen, um die Technik durch die beteiligten und betroffenen Parteien einschätzbar, gestaltbar und beherrschbar zu machen. Und umgekehrt die gesellschaftliche Reflexion in die innerfachlichen Diskurse zu integrieren. Dabei sollen im Rahmen dieser Arbeit, wie schon an der Ausgangslage ablesbar, vor allem die Verstrickungen von technischen, politischen und sozialen Aspekten des GNUnets in den Vordergrund geschoben werden.

Die Utopie und ihr Fehler

Warum aber mit dem GNUnet beschäftigen? Festzustellen ist, dass das GNUnet-Projekt seit mehr als einer Dekade, abgesehen von einigen Groschen öffentlicher Aufmerksamkeit, ansonsten wenig Ehre und Achtung erfahren hat. (Die Probe auf zwei Jahre, mit denen jedes Informatik-Projekt seine Eierschalen abzustreifen versucht, ist schon lange vorüber.) Vielleicht ist ja der Fehler, dass die Utopie nie wirklich ins Leben getreten ist – dann wäre es aber auch ihr einziger Fehler. Nach meinem Erkenntnisstand gibt es bisher keine Arbeit, die sich mit dem GNUnet nicht nur unter technischen, sondern auch unter gesellschaftlichen Aspekten auseinandersetzt.

»The Internet is broken, by design«,[10] schreiben die Wissenschaftler des GNUnet-Projekts im Jahre 2014. Das GNUnet-Projekt formuliert im Vergleich zu anderen ähnlichen Projekten wie dem Freenet-, Tor- oder I^{2}P-Projekt als einziges eine solche (wissenschaftlich praktizierte) Fundamentalkritik im Bezug auf die technisierten Formen der Informations- und Kommunikationsverarbeitung. Mir ist bewusst, dass dieser ernsthafte Versuch mit dem Potential, große Teile des Netzes zu reformieren, in Spannung steht mit der noch unbedeutenden Rolle des Projektes. Doch letztlich ist diese Arbeit und ihr zugrunde liegendes Problem von einem emanzipatorischen Erkenntnis- und Gestaltungsinteresse geleitet. Dem sei hinzugesetzt: Auch wenn die aktuellen Geheimdienstskandale einen weiteren schwerwiegenden

[10] Incipit von Grothoff et al. (2014).

Bewegungsgrund liefern würden, sind sie in meinen Augen historische Erfahrungen, die den Vorhergehenden an Bedeutung nichts nehmen, ja in der moralischen Entwürdigung der herrschenden Eliten ihresgleichen suchen. Das Nachdenken über Sinn, Herkunft, Zweck und Kontext der Technik ist eine genuine Aufgabe der Disziplin Informatik und Gesellschaft und soll dazu beitragen, die innerfachlichen Diskussionen anschlussfähig zu machen. Sie arbeitet reflexiv und am Puls der Zeit.

1.3. Zur Frage der Macht

Mit dem bisher Gesagten geht in dieser Arbeit die Annahme einher, dass sich das GNUnet-Projekt auch als ein politisches Vorhaben verstehen lässt, deren Interesse es ist, die (softwaretechnischen) Informations- und Kommunikationsinfrastrukturen als Mittel zum Zweck der Veränderung sozialer Verhältnisse neu zu konstruieren. Wenn nun jede Sozialordnung auf bestimmten Machtverhältnissen beruht, dann ist damit aber die Machtfrage implizit gestellt. Zwei Zuspitzungen sind dabei zu machen. Erstens werden nur diejenigen Formen der Machtausübung einbegriffen, die aus Sicht des GNUnet-Projekts als illegitim erscheinen, zweitens beziehen sich ihre Aktivitäten auf den sogenannten Informationsbereich. Beide bedürfen einer kurzen Erläuterung. Formen der Machtausübung als illegitim zu verdächtigen, setzt eine gewisse normative Vorstellung von Demokratie und/oder ethischem Verhalten voraus, wonach die Gegebenheiten korrekturbedürftig oder abzulehnen sind. Speziell im Bereich der Information, die als eine »Gesellschaft konstituierende Kategorie« (Steinmüller) gezählt werden darf, spricht man dann beispielsweise von Propaganda, Zensur, Kontrolle & Überwachung. Informationen sind hier der Gegenstand von Zensur, oder können im Fall von Kontrolle & Überwachung auch ein Mittel sein. Die Bedeutung der Legitimität wird eindrücklich, wo diese Praktiken rechtmäßig, aber möglicherweise moralisch fragwürdig sind.

Einer solchen Situation entspringt die Forderung nach Freiheit *von* Macht. Dem schließt sich auch das GNUnet-Projekt an. Das Narrativ hierfür liefert – wie wir noch sehen werden – der Diskurs der »Privacy- und Anti-Censorship-Technologien«. Dieser ist vornehmlich im amerikanischen Raum verwurzelt und hängt einer libertär-individualistischen Tradition an. Ich möchte untersuchen, auf welche Weise Macht-

verhältnisse umgestaltet werden und in welchen Bereichen dies geschieht. Dies wird uns Aufschlüsse darüber geben, wie weit sich die Risiken einer aus den Fugen geratenen Informationsmacht verringern lassen.

Es ist instruktiv für das Verständnis und eine Beurteilung seiner sozialen (und politischen) Veränderungsmöglichkeiten, das GNUnet-Projekt mit einer europäische Tradition zu kontrastieren: hierzulande geht der kritische Datenschutzdiskurs davon aus, dass es nicht um Privatheit geht, sondern um das strukturelle Problem, eine Technik sozial beherrschbar zu machen.[11] Martin Rost (2013a, S. 37) formuliert diese Kluft so: »Wo der Diskurs mit dem axiomatischen Ausgangspunkt der Selbstgenügsamkeit eines Monaden-Individuums allein auf den Abwehraspekt Bezug nimmt, verordnet er sich selbst eine Blindheit gegenüber der strukturellen Übermacht der Organisation.« Um es knapp zu sagen, bestand das Ausgangsproblem des Datenschutzprojektes (als gesellschaftliche Problemstellung) darin, das Verhältnis von gesellschaftlicher Macht und Informationsverarbeitung zu verstehen.[12] Mit diesem Verweis postuliere ich, dass sich beide Projekte im Grunde genommen dem gleichen Problem widmen. Dies werde ich versuchen, im Laufe dieser Arbeit plausibel zu machen.

Meine These ist nun: Erst im Kontrast mit dem Datenschutzprojekt gewinnt das Profil des GNUnet-Projekts Konturen, anhand derer sich bestimmte politische beziehungsweise gesellschaftliche Machtverschiebungen nachvollziehen lassen. Dort, wo mächtige soziale Akteure (a) vollständig berechenbare Internetdienste, also in Algorithmen vergegenständliche Handlungs- oder Arbeitsfunktionen (wie zum Beispiel Suchdienste) kontrollieren oder (b) die darunterliegende Internetinfrastruktdienste kontrollieren oder beeinflussen, können starke Machtverschiebungen zwischen den teilnehmenden sozialen Akteuren auftreten. Während im ersten Fall, so werde ich zeigen, durch das GNUnet die Organisationsmacht des Dienstleisters zersetzt wird, bedeutet es im anderen Fall, dass die Organisationsmacht von Kommunikationsdienstleistern auf die banale Funktion der (agnostischen) Paketvermittlung reduziert wird.

Allerdings gibt es Dienste (c), deren konstitutive Handlungs- und Arbeitsfunk-

[11] Vergleiche Wilhelm Steinmüller in ULD (2009).

[12] Ich danke Jörg Pohle, dass er mich früh auf diesen wesentlichen Punkt aufmerksam gemacht hat.

tionen *nicht* vollständig berechenbar sind oder von denen wir zumindest erwarten, dass beispielsweise menschliche Abwägungen ein Teil des Prozesses bilden sollten. Die Annahme oder Ablehnung eines behördlichen Antrags sollte eben keine Frage der Berechenbarkeit sein, auch wenn der Behördengang selbst elektronisch von statten geht. Zusätzlich zu dieser dritten Klasse gibt es eine vierte (d), nämlich digitale Infrastrukturdienste einschließlich ihrer Terminals, die als abgeschlossenes System vermachtet sind und infolgedessen ebenfalls keinen Machtverschiebungen des GNUnets unterziehbar sind. Gerade bei den letzten beiden genannten Dienstklassen ist das Problem der Informationsmacht, wie wir noch sehen werden, ein genuines Datenschutzproblem. Im Schlusskapitel werde ich anhand einer Topologie diese Machtverschiebungen systematisch veranschaulichen und erläutern.

2. Vorgehen

Die Kombination aus Datenschutz und Privacy-Technologien als Lösung der Machtproblematik im Informationsbereich weiter auszubuchstabieren, ist das Ziel dieser Untersuchung. Das Modell der Prozess-Domänen von Rost und Bock (2011) dient mir hierzu als Vorlage. Aber auch für die politischen und soziologischen Diskurse ergäbe sich ein klareres Bild über die Möglichkeiten und Grenzen dieser Technologie im Bezug auf Demokratie und Emanzipation. Und nicht zuletzt soll es auch dem GNUnet-Projekt helfen, eine mögliche Betriebsblindheit zu überwinden oder zumindest auf gesellschaftliche Aspekte aufmerksam zu machen, die aus der reinen Informatik schlicht nicht erfassbar sind. Mein Vorgehen sieht dafür folgendermaßen aus:

Um nicht den Boden unter den Füßen zu verlieren, gilt es zunächst einmal zu klären, wie die Technik verfasst ist. Wo die Informations- und Kommunikationsverarbeitung zunehmend in eine technisierte Form übergeht, stellt sich die Frage nach der Normativität der Technik überaus deutlich. In *Teil II* soll im engeren Sinne die Frage untersucht werden nach dem Selbstverständnis und dem Wertesystem des Projektes und wie sich diese in der Technik niederschlagen. Es liegt am Doppelcharakter technischer Regeln, sowohl zwingend regelmäßig als auch normativ

wirksam zu sein und dadurch den menschlichen Handlungsspielraum unter neue Bedingungen stellt.[13]

Läuft der vorherige Schritt also auf einen technologischen Begriff hinaus, werde ich in *Teil III* versuchen, die Machtverschiebungen als Folgenabschätzung zu beschreiben. Aufbauend auf einer näheren Begriffsbestimmung der Informationsmacht lassen sich hier zwei Typen von Machtverschiebungen unterscheiden: Erstens hinsichtlich der Kommunikationsverarbeitung und zweitens hinsichtlich der Informationsverarbeitung.

Mag es auf den ersten Blick erscheinen, als ob das Problem der Informationsmacht hinreichend erfasst ist, richte ich meinen Blick in *Teil IV* speziell auf Organisationen als soziale Strukturen mit gesellschaftlicher Funktion. In diesem letzten Schritt wird ein blinder Fleck offenbar, den ich damit entgegnen möchte, die Problemperspektive des Datenschutz- und des GNUnet-Projekts näher zu erkunden und einander gegenüberzustellen. Das Ergebnis ist ein Vorschlag, wie sich das GNUnet sinnvoll einordnen und beurteilen lässt.

3. Was ist ein P2P-Netz?

Um ein erstes Vorverständnis in der Annäherung an den Gegenstand meiner Arbeit zu bekommen, ist es nützlich, den technischen Überbegriff kennenzulernen. Was also ist ein P2P-Netz? Es handelt sich dabei um eine Netzwerkstruktur, die nach einem P2P-Modell entworfen wurde, bei dem im Allgemeinen Dienste und Funktionen dezentralisiert werden. Ein prominentes Beispiel für ein konkretes P2P-System ist der ehemalige File-Sharing-Dienst Napster: Jeder konnte an dem Netzwerk teilnehmen und Dateien mit anderen teilen. Zwar musste man erst auf einen *zentralen* Verzeichnisdienst nach Inhalten (MP3-Dateien) suchen und erhielt als Ergebnis die Adressen der Teilnehmer, die im Besitz einer Kopie dieser Inhalte waren. Aber

[13] In der Theorie der Informatik spiegelt sich dieser Umstand in dem Satz wider »Dekontextualisieren – Modellierung – Formalisieren – Operationalisieren – Automatisieren – Rekontextualisieren«, unter anderem nachzulesen bei Rolf (1992, S. 42. f.). Banse et al. (2006, S. 232, S. 110) weisen allgemeiner noch auf den institutionellen Charakter technischer Systeme hin: »Technische Sachsysteme wirken wie gesellschaftliche Institutionen, die menschliches Handeln in bestimmte Bahnen lenken.«

die Daten wurden *dezentral* über eine direkte Verbindung vom respektiven Peer kopiert.

Das Phänomen Napster war aufgrund seiner Popularität, seiner massenhaften Verwendung und – in Folge dessen – wegen der starken Auswirkungen auf den Informationsfluss im Internet zum Inbegriff von P2P-Systemen geworden und hat den Diskurs über P2P-Systeme seit den 2000er Jahren (auf eigentümliche Weise) maßgeblich geprägt.[14] Entscheidend war jedoch nicht die P2P-Idee als solche, sondern die Masse an neuartigen Peers, die an dem System teilnahmen und ihre ungenutzten Speicherressourcen zur Verfügung stellten: Personal Computers, die mit dem Internet verbunden waren.

In einer weiteren Annäherung lässt sich von einem P2P-Modell für ein Netzwerk sprechen, an dem Teilnehmer (Peers) nahezu gleichberechtigt teilnehmen und relevante Netzwerkdienste durch die Peers sowohl genutzt als auch zur Verfügung gestellt werden.[15] Client- und Server-Rolle verschmelzen im Peer und ermöglichen dadurch eine Form der Selbstorganisation des Netzwerkes, bei der unabhängig von der Anzahl der Peers die relevanten Dienste wie Datenspeicherung, Paketvermittlung oder Suchdienste von allen teilnehmenden Peers angeboten und gleichzeitig beansprucht werden können. Der Begriff der Rolle beinhaltet dabei zwei Facetten: Einerseits eine Menge von Rechten und Pflichten wie zum Beispiel Zugriffsrechte, Verteilrechte, Abfragerechte oder Weiterleitungspflichten, und andererseits ein Bündel von typischen Funktionalitäten beziehungsweise Fähigkeiten, die ein Peer gegenüber einem anderen Peer aufbringen kann und über ein Protokoll wechselseitig vermittelt werden. Technisch bedeutet dies, dass auf jedem Peer der gleiche Code läuft. Weicht ein Peer vom Protokoll ab, kann dies harte bis gar keine Sanktionen nach sich ziehen. Eines der besonderen Vorzüge von P2P-Netzwerken ist die gemeinsame Nutzung verteilter Ressourcen wie Speicherplatz, CPU-Leistung oder Bandbreite, die sich lokal auf den einzelnen Peers befinden.

[14] Historisch könnte das Internet als solches mit seiner dezentralen Architektur einen weitaus älteren und weiter verbreiteten Vorläufer darstellen. Mit der Übernahme der TCP/IP-Protokoll-Suite war es seit Mitte der 1970er Jahre technisch möglich, Netze mit neuen Knoten/Netzen zu verbinden. Diese Tatsache eines »offenen« Netzes hat unter anderem zu der Verbreitung der Internet-Infrastruktur beigetragen.

[15] Vergleiche Evans (2011, S. 7).

Abzuwägendes beim Entwurf von P2P-Systemen

Dezentrale Systeme haben gegenüber zentralisierten Systeme eindeutige Vorzüge, bspw. gemeinsame Ressourcennutzung, die Verteilung von Rechenleistung und Bandbreite oder eine höhere Zuverlässigkeit. Dies sind Merkmale, die P2P-Modelle bereits von ihrer Mutterklasse erben, den verteilten Systemen.[16]

Es gibt allerdings gute Gründe für P2P-Netzwerkarchitekten, wie GauthierDickey und Grothoff (2008, S. 1) anmerken, nicht alle Funktionen zu dezentralisieren: Leistungsfähigkeit (zu engl. Performance), Einfachheit, Kontrolle und insbesondere Sicherheit können bei der Abwägung eine Rolle spielen. Stellvertretend für diese Denkweise ist das zentralisierte Server/Client-Modell. In diesem Modell ist es technisch einfacher, Vertrauen zu modellieren, den Zugang zu beschränken, Ressourcen zu verwalten, Gebühren zu verlangen, Updates durchzuführen, Features hinzuzufügen oder zu entfernen.

Was den Aspekt der Sicherheit angeht, so gilt für reine P2P-Modelle, dass sie per Definition keine Infrastruktur-kritischen Punkte (zu engl. Single-Point-of-Failure) besitzen. Dennoch sind erhebliche Anstrengungen erforderlich, um die Sicherheits- und Zuverlässigkeitsprobleme in P2P-Entwürfen zu lösen, die sich aus dem Paradigma reiner P2P-Modelle selbst erst ergeben. Projekte wie das Freenet oder GNUnet legen Zeugnis davon ab.

Eine weiterer Aspekt ist die Kontrolle der Daten und ihrer Verarbeitung. Reine P2P-Modelle eröffnen die Möglichlichkeit, die Daten und die Verarbeitung ein Stück mehr unter die Kontrolle der Peers zu bringen. (Idealerweise sollte der Code auch einer Lizenz für Freie Software unterstehen, um diese Kontrollierbarkeit auch rechtlich zu gewährleisten.) Die Frage ist natürlich an dieser Stelle, welche Art von Daten und welcher Typ von Berechnungen unter welche Form von Kontrolle gebracht werden können. Diese Frage wird uns unter anderem in dieser Arbeit beschäftigen.

Der Preis für reine P2P-Systementwürfe ist trotz dieser wünschenswerten Vorzüge hoch: Sie sind intellektuell wie technisch schwierig zu entwickeln und, um sie hinsichtlich einer massenweisen und intensiven Nutzung zu testen, müssen große

[16] Vergleiche zum Beispiel Silberschatz et al. (2010, S. 673 ff.).

Netzwerke von Knoten simuliert beziehungsweise emuliert werden.

Nun kann man zwischen drei charakteristischen Klassen von P2P-Modellen differenzieren:[17] dem zentralisierten P2P-Modell, dem reinen P2P-Modell und dem P2P-Modell mit Super-Peers.

3.1. Zentralisierte P2P-Modelle

Charakteristisch für das zentralisierte P2P-Modell ist, dass für die Teilnahme bestimmte erforderliche Informationen an einen zentralen (autoritativen) Dienst übermittelt werden müssen. Ein Beispiel hierfür wäre wieder Napster, bei dem der zentrale Verzeichnisdienst die Peers verwaltet und Auskunft gibt, welcher Peer welche Inhalte zur Verfügung stellt. Das Beispiel zeigt, dass nicht alle Netzwerkfunktion (in diesem Fall der Verzeichnisdienst) dezentral sind.

3.2. Reine P2P-Modelle

Ein reines P2P-Modell ist ein Modell, in dem die Teilnehmer egalitär, das heißt mit symmetrischen Rollen, Rechten und Pflichten, teilnehmen und alle (wesentlichen) Netzwerkdienste durch das Zusammenspiel der Teilnehmer bereitgestellt und genutzt werden.[18] Charakteristisch ist ebenfalls, dass es keine koordinierende zentrale Autorität gibt und die Peers stattdessen alle das gleiche Protokoll befolgen. In einem solchen P2P-Modell hat kein einzelner Knoten mehr Macht beziehungsweise Kontrollmöglichkeiten als ein anderer. Das GNUnet gehört zu dieser Klasse.

3.3. P2P-Modelle mit Super-Peers

Das P2P-Modell mit Super-Peers ist charakteristischerweise eine Mischung aus einem reinen P2P-Modell und einem zentralisierten P2P-Modell, insofern wir zwei Klassen von Peers haben: Die sogenannten Super-Peers bilden zahlenmäßig die kleinere Klasse und haben typischerweise eine hohe Konnektivität zu den anderen

[17] Ich halte mich hier eng an die Topik von Evans (2011).

[18] Ich orientiere mich hier an einer Definition, die von Christian Grothoff in seiner Vorlesung vom 14. April 2013 gegeben wurde.

Super-Peers. Ihre Struktur entspricht dem eines reinen P2P-Modells. Ein Super-Peer ist auch der Eintrittspunkt für einen normalen Peer. Die Gruppe der normalen Peers bilden die überwiegende Klasse und es wird angenommen, dass diese Peers nur eine geringe Konnektivität besitzen und keine feste, global erreichbare Adresse haben. (Dies trifft zum Beispiel auf PC-Anwender mit einem handelsüblichen Internetanschluss zu.) Super-Peers müssen nicht nur eine höhere Konnektivität anbieten, sondern stellen in der Regel auch den Großteil der Ressourcen (wie z. B. Speicherdienste, VoIP-Dienste) zur Verfügung. Etwa in diesem Sinne sind sie die »zentralisierte« Komponente eines konkreten P2P-Systems.

Ein aktuelles Beispiel für dieses Modell ist der Voice-over-IP-Service Skype von Microsoft. Hier stellen Super-Peers den IP-Telefon-Service für normale Peers (Skype-Clients) zur Verfügung, in dem sie aufgrund einer festen IP-Adresse permanent erreichbar sind. Die normalen Peers speichern eine Host-Liste mit den Super-Peers, zu denen sie sich initial verbinden können. Die Kommunikation zwischen zwei normalen Peers wird üblicherweise über die Relay-Funktion eines Super-Peers ausgetragen. Eine Liste der verbundenen Skype-User wird dezentral von den Super-Peers verwaltet.

3.4. Underlay/Overlay-Netzwerke

Moderne P2P-Systeme werden als Overlay-Netzwerke entworfen und konstruiert. Damit ist eine inzwischen gängige Technik gemeint, die es P2P-Architekten ermöglicht, neue P2P-Protokolle und Anwendungen auf bereits bestehenden Netzwerken zu betreiben, ohne den bestehenden Protokoll-Stack im Betriebssystem eines Hosts zu verändern. Ein Underlay-Netzwerk bezeichnet entsprechend das darunterliegende Netzwerk, zum Beispiel das Internet mit seiner TCP/IP-Suite.

Derartig vorbereitet soll nachfolgend das P2P-System GNUnet analysiert werden, um das technische Verständnis zu erlagen, das für die Bewertung ihrer sozialen Auswirkungen nötig sein wird.

Teil II.
Analyse: Was ist das GNUnet?

1. Selbstbild des GNUnet-Projektes

Ich beginne mit einer ersten formalen Unterscheidung unterhalb des obersten Diskurssignifikanten »GNUnet«: Wenn vom GNUnet-»Projekt« die Rede ist, so ist damit nicht nur die unter technisch-organisatorischen Bedingungen entstehende Software gemeint, sondern eben auch die Forschungsgruppe »Free Secure Network System Group« der Technischen Universität München und der lose Verbund von teilhabenden engagierten Entwicklern. Der Kern der Forschungsarbeiten wird seit 2015 an der französischen Universität Inria innerhalb des »Equipe Décentralisé« fortgesetzt.

Das GNUnet-»System« hingegen umfasst die technischen Modelle (für dezentrale Dienste und sichere Protokolle), die entwickelte Codebasis und die Binärdateien. Schließlich sei das »GNU network« oder einfach »GNUnet« die Bezeichnung für ein Netzwerk aus digital vernetzten Rechnern (Hosts), auf denen die GNUnet-Software ausgeführt und von partizipierenden Nutzern betrieben wird.

Die Frage, die uns nun zuvorderst interessiert, ist die nach dem Selbstbild und der Identität des Projektes. Einerseits sind Identitäten sinnstiftend und definieren auf einer abstrakten Ebene ein Kriterium der Gruppenzugehörigkeit. Wer sich identifiziert, teilt beispielsweise die Ziele und Ideale, die im Selbstbild zum Ausdruck kommen und stimmt sein Handeln auf diese ab. Beginnen wir mit dem folgenden Satz als Manifestation des Selbstbildes:

> »The foremost goal of the GNUnet project is to become a widely used, reliable, open, non-discriminating, egalitarian, unfettered and censorship-resistant system of free information exchange. We value free speech above state secrets, law-enforcement or intellectual property. GNUnet is supposed to be an anarchistic network, where the only limitation for peers is that they must contribute enough back to the network such that their resource consumption does not have a significant impact on other users.«[19]

Diese Aussage ist ergreifend und scheint den Nerv der Zeit sogar ein wenig überzustrapazieren. Warum? Neben einer Reihe von Werten (offen, nicht-diskriminierend, egalitär, ungehindert, zensurresistent), die im modernen Staatsverständnis mehr

[19] Im Internet: https://gnunet.org/philosophy, Stand: 25.7.14.

oder weniger als anerkannt gelten können, ist wohl der herausragendste Punkt das Recht auf freie Meinungsäußerung und Informationsaustausch. Die Schärfe steckt jedoch in ihrer staatskritischen Haltung, die freie Meinungsäußerung höher wertzuschätzen als die gegenwärtig weit verbreiteten rechtsstaatlichen Elemente des Staatsgeheimnis, der Strafverfolgung oder des »geistigen Eigentums«.[20]

Hinzu tritt die Leitidee eines anarchistischen Netzwerkes. Im Alltagsgebrauch wird Anarchismus mit der Ablehnung des Staates, Gesetzlosigkeit, Chaos und Gewalt in Verbindung gebracht. Eine etwas nähere Bestimmung aus den politischen und philosophischen Diskursen würde versuchen, entlang der Figuren der unbegrenzten Freiheit des Individuums oder der Herrschaftsfreiheit zu arbeiten. Die Bedeutung besteht darin, dass sich das Individuum von Autoritäten jeglicher Art befreit, »seien sie ideologischer Art (Religion, politische Doktrinen usw.), institutioneller Art (Staat, Bürokratie usw.), ökonomischer Art (privates und öffentliches Eigentum), sozialer Art (Klassen-, Stände- oder Kastenzugehörigkeit) oder auch juristischer Art (legislativer und normativer Apparat)«.[21] In einigen anarchistischen Strömungen sind Formen der Selbstorganisation erstrebenswert, so dass die vom GNUnet-Projekt genannte Regel »genügend Ressourcen zur Unterstützung des Netzwerkes bereitzustellen« als Voraussetzung eines konsensualen Prozesses verstanden werden kann.

Der Zweck des GNUnet-Projektes ist von Grothoff (2011) auf eine prägnante Formel gebracht worden, und zwar die Möglichkeiten und Grenzen von sicherer Peer-to-Peer-Kommunikation zu erforschen. Weitläufiger lautet das Bestreben des GNUnet-Vereins, die »Sicherheit im Internet für alle Bürger mittels freier Software, Dezentralisierung von Diensten und sichere Netzwerkprotokollen durch Forschung, Entwicklung und Bildungsangebote zu fördern«.[22]

Für meine weitere Untersuchung zur Normativität der Technik werde ich mir diese Selbstdarstellung als Einstiegspunkt zu Nutze machen. Dabei operiere ich mit dem »Vorbehalt gegen die Selbstauslegungen von sozialen Gebilden und Individu-

[20] Die korrekte Bezeichnung wäre immaterielle Güter. Der Kontext legt jedoch nah, dass hier die Konfliktlinie innerhalb der Eigentumsverhältnisse gemeint ist.

[21] Rehfus (2003, Anarchie).

[22] Aus der Satzung des GNUnet e.V. in der Fassung vom 20.9.2013. Im Internet: https://gnunet.org/svn/gnunet-ev/satzung.tex.

en« (Jaeggi, 2009b), indem ich weitere Erkenntnisquellen wie Schriften, Vorträge, Foreneinträge oder IRC-Beiträge hinzuziehe. Zwar erschließt sich aus der facettenreichen Selbstdarstellung nur ein oberflächliches Bild über die normative Praxis, aber sie verrät uns gewissermaßen Ansatzpunkte, an denen eine normative Rekonstruktion der entscheidenden Werte auszurichten ist. Meine Vermutung ist, dass die Werte des Privaten und des Antiautoritären, wie ich sie nennen möchte, von herausragender Bedeutung sind.

2. Werte und Wertvorstellungen des GNUnet-Projektes

Werte prägen Handlungsorientierungen. Wer ein Stück Code schreibt und dabei »Wert« auf die Korrektheit der Berechnung legt, damit das Programm keine falschen Ergebnisse zurückliefert und der Kühlschrank nicht ”-1” Packungen Milch bestellt, trifft beim Programmieren an unterschiedlichen Stellen Wertentscheidungen. Dort, wo Gestaltungsspielräume bestehen und anders gehandelt werden kann, entfalten Werte ihre normative Kraft, sich für das eine und gegen das andere zu entscheiden. Zudem gilt, dass ein Wert in Gegenwart konkurrierender Werte innerhalb der Gesinnung eines Menschen oder einer Gruppe abgewogen werden muss. Mitunter können die daraus folgenden Entscheidungen andere Menschen betreffen (wenn diese zum Beispiel den Code ausführen), so dass eine ethische Dimension zum Vorschein kommt. Wird diese Dimension berücksichtigt und reflektiert, kann man davon sprechen, dass ethische Werte die Entscheidungen beeinflusst haben. Dies bedeutet, dass man einer allgemeinen Auffassung nach ethische Werte nicht nur mit anderen Menschen teilen, sondern ihnen über die Ausführung von Code Geltung verschaffen kann. Und genau um diese Art von Werten mit zwei Gesichtern soll es im Folgenden gehen.

Das GNUnet-Projekt erschafft durch den produzierten Code einen »sozialen Rahmen« mit Regeln, die keinen vernehmbaren sozialen Theorien entspringen, sondern aufgrund von Wertentscheidungen (und den um sie herum gebildeten informatischen Modellen) zustande kommen. Aber wie sehen die dahinterstehenden

Wertvorstellungen aus? Und wie schlagen sich diese in der Technik nieder?

2.1. Der Wert des Privaten

Aufbauend auf den Forschungsarbeiten von Seda Gürses, Claudia Díaz und George Danezis möchte ich zeigen, dass das GNUnet-Projekt dem Privacy-Paradigma »Privacy as Confidentiality« untersteht und der Wert des Privaten daher einen großen Einfluss auf das Projekt hat. Dies möchte ich zum einen durch die Herstellung eines historischen Zusammenhangs leisten und zum anderen, indem ich die charakteristischen Merkmale des Privacy-Paradigmas im GNUnet-Projekt identifiziere. Der Mehrwert besteht darin, dass uns dieser in Relation gebrachte Privacy-Begriff erlaubt, ihre ideologischen Grundlagen trotz der fehlenden Selbstauseinandersetzung etwas besser zu begreifen. Privacy wird damit aber auch als ein Wert verstehbar, an dem sich die (sozialen) Praktiken orientieren.

Gemäß dem historischen Narrativ des selbstkritischen[23] Privacy-Diskurses war es Chaum (1981), der Ende der 70er Jahre die ersten Vorschläge für anonyme Kommunikation im Kontext überwachter Netze vorlegte und damit das Feld der »Privacy-Technologies« (PT) bestellte. In der Folge bildete sich in den 80er Jahren kleine Gruppen von Forschern (u. a. die Gruppe um Andreas Pfitzmann), die von diesen Ideen beeinflusst waren und die Möglichkeiten anonymer bzw. vertraulicher Kommunikation zu erforschen begannen. Unter Vertraulichkeit verstand man einerseits die Geheimhaltung von kommunizierten Inhalten und andererseits die Geheimhaltung von Information, welche Teilnehmer zu welcher Zeit miteinander kommunizierten – beides gegenüber nicht autorisierten Anderen. Erneut war es Chaum, der Mitte der 80er die paradoxen Konzepte Authentisierbarkeit und Anonymität mittels digitaler Pseudonyme zusammenbrachte. Auf dieser Basis wurden bis in die 90er kryptographische Konzepte wie »blind signatures«, »selective disclosure credentials« oder »zero knowledge proofs« hervorbrachte. Die PT-Gemeinschaft wuchs seit den 2000er Jahren rasant an, und es sind jene Jahre, in denen eine Viel-

[23] Die Ausgangsfrage lautet: »The debate needs to be robust and ambitious, and not shy away from uneasy questions, including ›is privacy even the right point of departure to think about developing counter-surveillance technologies?‹«, Danezis und Gürses (2010, S. 2).

zahl der heutigen PT-Projekte ihre ersten Kinderschritte wagten. Erklärt wird dies vor allem mit zwei Institutionalisierungs-Maßnahmen: der Einrichtung des Privacy Enhancing Technologies Workshop (PETW) und des ACM Workshop on Privacy in the Electronic Society (WPES).

Aufbauend auf dieser Darstellung identifizieren Danezis und Gürses (2010) eine liberal-individualistische Strömung, die sich die erstaunlich kurze Privacy-Definition von Warren und Brandeis (1890) zu Nutze macht: »the right to be let alone«. Unterhalb dieser Definition konzeptionalisieren sie ein Paradigma, das sie als »Privacy as Confidentiality« bestimmen. Es zeichnet sich dadurch aus, eine »individuelle und autonome Sphäre« erschaffen zu wollen, die den Einzelnen vor den »Übergriffen« des Staates oder dem »Druck sozialer Normen« schützen soll. Die darin enthaltene liberal-individualisitisch Vermutung und philosophische Grundthese ist mit Raymond Geuss (2013, S. 111) gesprochen vielleicht diese, dass der »beste Weg, die Individuierung und selbstbestimmte Entfaltung zu fördern, darin besteht, völlige Privatheit zu gewährleisten«.

Übertragen auf den digitalen Informations- und Kommunikationsbereich sollen Informationsdienste nutzbar sein, ohne dabei persönliche Informationen offenzulegen beziehungsweise bei minimaler Offenlegung keine Rückschlüsse auf ein Individuum zu erlauben. Die Gefahr, die von den Befürworten gesehen wird, besteht in der Sammlung und Verknüpfbarkeit von Informationen zum Zwecke der Überwachung, der Profilbildung und der Manipulation. Was sind nun die Merkmale dieses Paradigmas?

1. »›Privacy‹ wird formalisiert«: Privacy-Konzepte werden als Privacy-Eigenschaften formal definiert und mittels begleitender Sicherheitsprüfungen auf ihre Geltung fortwährend geprüft. Wo rechtliche Normen versagen, sollen technische Normen die Schutzgüter von Privacy bewahren.

2. »Informationsoffenlegung vermeiden«: Der Fokus liegt darauf, zu verhindern, dass Informationen offengelegt werden. Das Credo lautet: Sind persönliche Informationen erst einmal offen zugänglich, ist die individuelle und autonome Sphäre nahezu unwiderruflich durchbrochen.[24]

[24] Vergleiche Danezis und Gürses (2010, S. 4).

3. »Vertrauen minimieren«: Jede Möglichkeit vermeiden, einem anderen die Handhabung identifizierbarer oder verlinkbarer Daten anzuvertrauen.

Exemplarisch für dieses Paradigma sind Techniken vom Typ »Anonymous authentication protocols«, »Anonymous communication networks« und »Private Information Retrieval (PIR)«.[25]

Wie hängt dieses Paradigma nun mit dem GNUnet-Projekt zusammen? Historisch ist das GNUnet-Projekts aus der Traditionlinie der PTs, wie ich sie oben wiedergegeben habe, hervorgegangen. Wichtige technische Impulse für diese signifikante Vergrößerung in den 2000er Jahren gaben der »Eternity Service« von Anderson (1996), der den Zusammenhang zwischen verteilten Speichern und Zensurresistenz herstellte,[26] und das »Free Haven«-Projekt von Dingledine et al. (2001), das anonymes verteiltes Speichern und Zensurresistenz zusammenbrachte.[27]

Das erste GNUnet-System war eine anonyme, verteilte File-Sharing-Anwendung, die ein zensurresistentes Kodierungsschema verwendete. Aus den Schriften, die zwischen 2002 und 2003 entstanden sind und dieses System beschreiben, finden sich Referenzen auf Vorgänger- und Nachbarprojekte. Der Abarbeitungs- und Lernprozess fand an den verschiedensten Projekten für verteiltes File-Sharing in P2P-Netzen statt, doch den größten Kampfplätze bildeten freilich anonymisierende Protokolle und zensurresistente Systeme.

Einschlägig hierfür sind die Referenzen in der Schrift über »GAP – practical anonymous networking« von Bennett und Grothoff (2003) und in der Schrift »An Encoding for Censorship-Resistant Sharing« von Grothoff et al. (2003). Im ersten Fall werden die Protokolle DC-Net, Mixer, Onion-Routing, Crowds, Hordes und P5 referenziert, da sie Anonymitätsaspekte erfassen, im zweiten Fall die Systeme Freenet, Freehaven, Mnet, MojoNation, Tangler, Gnutella und Fasttrack, da sie zensurresistente Eigenschaften besitzen.

1. Merkmal

Dieser Zusammenhang ist ebenfalls mit Blick auf die Merkmale des Paradigmas gegeben. Gemäß dem ersten Merkmal (»›Privacy‹ wird formalisiert«), wird das Schutzziel Privacy in Form von Angreifermodellen reformuliert, in denen die

[25] Díaz und Gürses (2012, S. 3).
[26] Danezis und Díaz (2008, S. 12).
[27] Danezis und Díaz (2008, S. 2).

persönlichen Daten das Schutzgut sind.[28] Dabei kommen die aus der Informationssicherheit stark formal definierten Schutzziele Vertraulichkeit (Confidentiality), Anonymität *(Anonymity)*, Abstreitbarkeit (Deniability) oder Zensurresistenz (Censor-resistance) von digitalen Inhalten und schließlich Authentisierung (Authentication) in Anonymitätsprotokoll zum Einsatz. Ein Reduktionismus, der sich unmerklich vollzieht und es nun erlaubt, diese Eigenschaften auf technisch bekannte Sicherheitsprotokolle und kryptographische Algorithmen abzubilden.[29] Sie sind bis heute Schlüsselkonzepte des GNUnet-Projekts.[30]

2. Merkmal

Für das zweite Merkmal (»Informationsoffenlegung vermeiden«) führe ich repräsentativ die Textstelle bei Bennett et al. (2002a, S. 2) an. Dort wird die Offenlegung der Aktionen der Nutzer als auch deren Identitäten als Makel bestehender Entwürfe bewertet. Die Idee der Vertraulichkeit beziehungsweise Geheimhaltung personenbezogener Daten, wie wir sie in den 1980er Jahren vorfinden, werden hier also fortgeführt und spiegeln sich bis heute in den oben genannten Schlüsselkonzepten wider.[31]

3. Merkmal

Und schließlich ist das dritte Merkmal (»Vertrauen minimieren«) durch das vom GNUnet-Projekt allgemein verwendete Angreifermodell bzw. Vertrauensmodell gegeben: Jede Systemkomponente wurde nach der obersten Maßgabe entworfen, dass es keine »vertrauenswürdige Autorität« geben darf, da sie das System angreifbar macht und damit personenbezogene Informationen Preis gibt. Dazu die folgende frühe Textstelle:

> »Any kind of central server would open the network to attacks, whether by attackers trying to control these entities, legal challenges, or other threats which might force operators of such critical and exposed nodes out of business. The best way to guard against such attacks is not to have any centralized services.«[32]

[28] Siehe beispielhaft Bennett und Grothoff (2003, S. 3), Grothoff et al. (2003, S. 2, 17). Zeitgenössische Referenzen sind Evans (2011, S. 149) oder Grothoff (2013, Folie 4).

[29] Faktisch wurde das Feld der Privacy-Technolgies vor allem durch Computer-Sicherheits- und Kryptographie-Experten geprägt.

[30] Im Internet: `https://gnunet.org/concepts`, Stand: 6.12.2014.

[31] Dieses Konzept war bereits in den 1960er ein herrschendes Modell in der Informatik, siehe Petersen und Turn (1967). Für diesen Hinweis danke ich Jörg Pohle.

[32] Bennett und Grothoff (2003, S. 2).

Dieses Merkmal ist bis heute weiterhin zentral, siehe auch Grothoff et al. (2014, S. 5). Kryptographische Algorithmen, sichere Protokolle, aber auch die Sicherheit des Endnutzersystem bilden die neuen *lokal* verorteten Vertrauensanker.

Das Signum »Privacy« ist zu einem Geburtsmerkmal des GNUnet-Projekts geworden und es durchzieht bis heute auf spezifische Art und Weise die Software-Architektur und ihre Mechanismen.

2.2. Der Wert des Antiautoritären

Aus der oben angeführten Passage bezüglich der Selbstauslegung nehme ich die Idee eines anarchistischen Netzwerkes als nächsten Anknüpfungspunkt, um einen zweiten konstitutiven Wert herauszuarbeiten. Um es gleich vorweg zu nehmen: Die Besonderheit dieses Wertes besteht darin, dass er eine andere Logik im Entwurfsprozess entfaltet oder bewirkt, die nicht in Deckung zu bringen ist mit der Logik des Privaten. Man könnte den hier zur Diskussion stehende Wert als Idee der Gleichheit bezeichnen. Aber damit würde es dem GNUnet-Projekt seine kämpferische und politische Schärfe rauben, weshalb ich mich für den Begriff des Antiautoritären entschieden habe. Nicht zuletzt verweist diese negative Formulierung auf strukturelle Unterordnung und Unterdrückung als wesentliche Motive der dahinterstehenden Wertvorstellung. Nachfolgend möchte ich versuchen, eine plausible Begründung für sein Vorhandensein zu geben. Dafür beginne ich mit einer kurzen Begriffsklärung und führe anschließend Indizien an, an denen sich diese vorherrschende Wertvorstellung im Projekt aufspüren lässt.

Begriff

Der Begriff des Antiautoritären, wie ich ihn verstehe, beinhaltet im Kern die Ablehnung von Autoritäten und die Wertschätzung herrschaftsfreier Verhältnisse unter Menschen. Autoritäre Verhältnisse zwischen Menschen werden durch ein hierarchisches Verhältnis begründet, dem zwischen Übergeordneten (Autorität) und Untergeordneten, jenem, der Anweisungen erteilt, und diesem, der gehorsam Folge leistet und die Anweisung über seinen Körper, sein Leben, seine Arbeit entgegen nimmt. Doch erst wenn dieses Unterordnungsverhältnis als Unterdrückungsverhältnis artikuliert wird, bei dem das Recht einer Subjektposition (bspw. ethnische, regionale, sexuelle Minderheiten) untergraben wird, konstituiert sich ein autoritäres

Verhältnis. Diese werden, wie Alex Demirović (2014, S. 18) schreibt, durch Gehorsamsproduktion, wie man sie »in Bereichen wie Kindergarten, Schule, Hochschule, Familie, Fabrik oder Gefängnis« findet, innerhalb der Gesellschaft reproduziert und reichen bis zur staatlichen Ebene in Form eines »autoritären Legalismus, wie er im Grundgesetz fixiert wurde. Diesem zufolge definieren Legislative, Exekutive und Judikative, was das Allgemeine ist, woran sich die Bürgerinnen [und Bürger] dann zu halten haben. Denn es soll sich ja um ihr Parlament, um ihre Repräsentantinnen [und Repräsentaten] handeln.«

Ich nehme als erstes den Vortrag von Christian Grothoff als Wortführer und Leiter des GNUnet-Projekts zum Anlass, diese Untersuchung durchzuführen. In seinem Vortrag »Tools for Breaking out of PRISM«[33] (2014) zeigt er ausgehend von verschiedenen historischen Beispielen und den Reaktionen aus der Politik die Alternativlosigkeit *in* der Politik. Er zählt dazu die Enthüllungen zum globalen Überwachungssystem auf (PRISM, X-Key-Score, Boundless-Informant); die Irak-Kriegsaffäre von 2003, bei der sechs Delegationen der Vereinten Nationen durch die US-Behörden politisch bespitzelt wurden, um auf jedwede »Überraschungen« vorbereitet zu sein; die geheime offensive »Cyberwar«-Politik der USA, der schlicht nationale Sicherheitsinteressen zugrunde liegen; das Echelon-Projekt als ein Vorläufer des bestehenden Überwachungssystem u. a. zum Zweck der Wirtschaftsspionage; und die staatliche Kooperation mit High-Tech-Unternehmen wie Microsoft als integraler Bestandteil dieser Systeme. Er stellt daraufhin fest, dass die Reaktionen seitens der Politik in zweierlei Hinsicht fatal sind:

Einerseits haben die US-Amerikaner nicht nur ein Problem, ihre Dienste unter Kontrolle zu bringen,[34] sie sind auch von der Doktrin der nationalen Sicherheit geleitet. Andererseits besteht auf Seiten der politischen Eliten Europas ein starkes Interesse, sich in das amerikanische System der Überwachung einzugliedern.[35] Er

[33] Im Internet: https://www.youtube.com/watch?v=1lcauMH70cA, Stand: 16.12.14.

[34] Dies macht er an dem symbolischen Ereignis fest, als der Geheimdienstdirektor James Clapper vor dem US Senate Intelligence Committe Rede und Antwort stand bezüglich der Frage, ob die NSA Massenüberwachung betreibe – seine Antwort war »No, Sir«.

[35] Grothoff zitiert hierzu ein Gutachten aus dem Jahre 1998, aus dem hervorgeht, dass das EU-Staaten 1995 im geheimen beschlossen haben, ein Überwachungsnetzwerk zu installieren, und zwar mit engen Verbindungen zum amerikanischen Inlandsgeheimdienst FBI.

zog daraus die unweigerliche Konsequenz, dass *politische Lösungen nicht zu erwarten seien.* Es ist daher nicht verwunderlich, wenn er in seinem Vortrag auf dem 30. Chaos Communication Congress Ende 2013 diesen Zustand im gleichen Atemzug mit den humanitären Katastrophen der Gegenwart erwähnt. Sein Engagement richtet sich gegen autoritäre Regime und Organisationen, und insofern sie Teil eines herrschenden politischen Systems sind, werden auch keine politischen Lösungen erwartet.

Politischer Kontext

Dieses generalisierende Urteil ist in gewisser Weise symptomatisch für unsere Zeit und lässt sich mit der politischen Diagnose Colin Crouchs in Beziehung setzen, dass wir in einem postdemokratischen Zustand leben. Heute gilt sein Begriff der Postdemokratie als Grundlage für die Kritik des Neoliberalismus. Die postdemokratische These besagt, dass »[w]ährend die demokratischen Institutionen formal weitherin vollkommen intakt sind (und heute sogar in vielerlei Hinsicht weiter ausgebaut werden), entwickeln sich politische Verfahren und die Regierungen zunehmend in eine Richtung zurück, die typisch war für vordemokratische Zeiten: Der Einfluss privilegierter Eliten nimmt zu, in der Folge ist das egalitäre Projekt zunehmend mit der eigenen Ohnmacht konfrontiert.«[36] Die Symptome reichen von erodierenden demokratischen Institutionen (z. B. in der allgemeinen Form eines Abbaus des Sozialstaats), über einem starken Lobbyismus global operierender Unternehmen bis zur Wiederkehr vom Modell des Nachwächterstaates mit einem starken polizei- und geheimdienstlichen Apparat (um den wirtschaftlichen Handel und die Eigentumsverhältnisse zu sichern).

Reaktionen

Es gibt auf diesen postdemokratischen Zustand verschiedene allgemeine Reaktionen, die sich als Versionen einer »Negation der Politik« verstehen lassen können. Dabei meint die Negation der Politik eine Strategie des Widerstandes, die sich diesem Zustand zu entziehen und Freiräume zu schaffen versucht. Innerhalb der Diskurse über »Privacy- und Anti-Censorship-Technologies« könnte man die folgende typische Positionen hervorheben:

1. Die vollkommene Ablehnung des staatspolitischen Rahmens aufgrund seiner paternalistischen und unterdrückenden Natur und der Bezug auf die Mög-

[36] Crouch (2008, S. 13).

lichkeit, durch Privacy-Techniken staatsfreie Räume im Internet zu schaffen (»Cyber-Anarchismus«-Bewegung der 1990er);[37]

2. Die Anerkennung des staatspolitischen Rahmens unter der Bedingung, überhaupt keine persönlichen Daten zu erheben, zu speichern und zu verarbeiten, und zwar aufgrund ihrer unkontrollierbaren ausufernden Gewalt gegenüber dem »Recht auf Privacy« (akademische und bürgerrechtliche Bewegungen, die dem o. g. Privacy-Paradigma unterstehen).

3. Die Anerkennung des staatspolitischen Rahmens und der auf Personenregistern basierenden Verwaltungsfunktionen unter der Bedingung, allgemeine Formen der totalen Überwachung zu verhindern (akademische und bürgerrechtliche Bewegungen aus den Surveillance Studies).

In seiner Erzählung schildert Levy (2000, S. 210 f.), wie nah sich die beiden ersten Haltungen Mitte der 1990er waren und sich entsprechend beeinflusst haben (als »Cypherpunks« wurden Personen aus beiden Lagern bezeichnet, ihr Kommunikationsmedium waren die anonymen Cypherpunk-Remailer). Diese Verstrickungen sitzen tief, auch wenn sich das GNUnet-Projekt der zweiten, bereits oben geschilderten Traditionslinie zuordnen lässt. Aber allgemein kann die Negation der Politik als eine Begründung dienen, ein Nährboden für die Herausbildung des Werts des Antiautoritären zu sein, einer kritischen bis ablehnenden Haltung gegenüber Organisationen wie dem Staat.

Nehmen wir zwei weitere Indizien, um diesen Wert herauszustellen. Grothoff ist nicht nur Haupt-Maintainer des GNUnet-Quellcodes, er ist auch Wortführer des Projektes und wissenschaftliche Leitfigur, der in seinen Seminaren u. a. zwei kritische Lektürehinweise gibt:[38] »The Authoritarians«, ein Buch von dem amerikanischen Psychologen Bob Altemeyer (2006), der für seine Forschung im Bereich der behavioristischen Autoritarismus-Studien bekannt ist. Dieses Werk versucht

[37] Siehe dazu auch Levy (2000, S. 206). Vertreter dieser Position wie John Perry Barlow haben ihren Irrtum beziehungsweise ihre Illusion eines rechtsfreien Raums erkannt.

[38] Im Internet: http://grothoff.org/christian/teaching/2014/2194/, Stand: 16.12.2014.

autoritäre Akteure zu identifizieren, ihr Wesen und die Ursachen für ihre Aggressionen zu bestimmen. Ein anderes Buch trägt den Titel »Seeing Like a State: How Certain Schemes to Improve the Human Condition have failed« und stammt vom amerikanischen Politikwissenschaftler und Anthropologen James C. Scott (1999). Es ist von der Beobachtung geleitet, dass Staatsapparate in einem historischen Prozess die Standardisierung und Rationalisierung soweit vorantrieben, dass sie die komplexen, lokalen sozialen Praktiken durch vereinheitlichende Transformationen zur besseren Kontrolle unterdrückten.

Zum zweiten Indiz: Diese Wertvorstellung drückt sich aber auch auf fundamentale Weise in den konkreten Arbeiten des GNUnet-Projekts aus, nämlich in der technischen Gestaltung als Prinzip der Dezentralisierung und Hierarchielosigkeit. So steht bei Grothoff et al. (2014, S. 5) mit Blick auf das technische Produkt des GNUnet-Projektes:

> »We must seize the opportunity to build a better network. [...] Most importantly, our design avoids hierarchical structures, ›trusted‹ authorities or central points of failure, as those will be exploited by authoritarian organizations and thus contribute to the collapse of civil society.«

Alle Entwicklungsarbeiten der letzten zehn Jahre innerhalb des GNUnet-Projektes werden diesem Gestaltungsprinzip, so weit es möglich ist, unterworfen.

Ein abschließendes Indiz soll die staatskritische Position des GNUnet-Projektes vor Augen führen. Vor dem Europarat machte Grothoff am 28.1.2014 deutlich, wogegen sich sein Interesse richtet, und zwar gegen die Möglichkeiten der Überwachung und Verletzbarkeit der Gesellschaft und des Individuums durch Staat und Wirtschaft als mächtige Gesellschaftsakteure. Er plädierte dafür aufzuhören, propietäre Software zu benutzen, und diejenigen Gesetze abzuschaffen, die Vorratsdatenspeicherung und Überwachung der Telekommunikation ermöglichen.

Die bisher aufgegriffenen Punkte zeigen auf unterschiedlichen Ebenen Bezüge auf zu Themen wie Hierarchie, Bevormundung, Unterordnungs- und Unterdrückungsverhältnissen, wobei in den meisten Fällen eine staatliche oder wirtschaftliche Organisation als Verursacher hervorgehoben wird. Mein Vorschlag an dieser Stelle ist daher, diese Reihe sinnvoll unter dem Wert des Antiautoritären zusammenzu-

fassen. Im Unterschied zum Wert des Privaten, der (als Kurzformel ausgedrückt) Handlungen einer Praxis der Geheimhaltung zuführt, geraten beim Wert des Antiautoritären Strukturen und ihre gemeinschaftliche Funktion in einen ethischen Diskurs über ihre richtige Verfasstheit. Dieser Wert leitet zu einer Praxis der Vermeidung von Autoritäten an, bei der Wertentscheidungen über die Frage des einseitigen Missbrauch dieser Strukturen produziert werden.

Wie aber finden die Werte des Privaten und des Antiautoritären Eingang in die technisch-wissenschaftliche Praxis und den technischen Substrat? Im Folgenden werde ich einige Überlegungen zu den verwendeten Modellen anstellen, die sich nach diesen Werten ausrichten oder zu ihrer Verwirklichung beitragen.

2.3. Modelle als normative Wertausprägungen

Angreifermodell

Ein weit verbreiteter Methodenansatz, der in dem oben genanannten Privacy-Paradigma auftaucht, ist von Computersicherheitsforschern und Kryptographieexperten aus dem militärischen Kontext übernommen worden. Er besteht darin, Angreifer-, Gefahren- oder Vertrauensmodelle zu formulieren und in konkrete Systementwürfe zu gießen.

Das Angreifermodell des GNUnet-Systems ist im Allgemeinen anspruchsvoll, da es für die meisten seiner Module als potentielle Angreifer sogenannten »Advanced Persistant Threats« (APTs) annimmt. APTs sind die dunkle Quelle für Bedrohungen, Gefahren und schadensträchtige Aktionen. Es handelt sich hierbei um ein Modell eines mächtigen Akteurs in der Rolle eines Angreifers, der über viele Ressourcen verfügt und dem besonders gefährliche beziehungsweise schadensträchtige Handlungsmöglichkeiten im Verhältnis zu anderen Akteuren zugeschrieben werden. Ein solcher potenter Angreifer könnte beispielsweise der Staat sein.[39] Charakteristisch für diesen Angreifer ist, dass er (a) jede Rolle in dem System annehmen kann (z. B. als Staat, Unternehmen oder Individuum), (b) verschiedene Identitäten annehmen kann (z. B. mehrere GNUnet-Hosts kontrollieren mit unterschiedlichen Identitäten),

[39] Vergleiche zum Beispiel Wachs et al. (2014, S. 3).

(c) in der Lage ist, sehr viele Rechenressourcen einzusetzen, (d) und über »rechtliche Macht« verfügt (z. B. um sich legal private Krypto-Schlüssel aushändigen zu lassen).[40] Das Angreifermodell lässt also zu, dass bösartige Peers am System teilnehmen können und damit zu einem »berechenbaren« Faktor werden. Popkulturell entspricht dieses Akteursmodell in etwa den Agenten im Film »Matrix« von den Wachowski-Brüder. Die Heldenfigur Neo wird hier gewarnt, dass jeder, dessen Stecker nicht gezogen ist, ein potentieller Agent des Systems ist.

Natürlich ergibt sich das konkrete Gefahren- und Angreifermodell und dazugehörigen Sicherheitsmaßnahmen erst aus der konkreten Anwendung/Submodul innerhalb des GNUnet-Systems. Aber die Abwehr eben jenes potenten Angreifers als größte Gefahrenquelle ist als Ausgangspunkt allen Modellen gleich. Das Angreifermodell des »GNUnet Anonymity Protocol« (GAP) nimmt z. B. an, dass ein Peer anonym operieren kann, auch wenn es keine vertrauenswürdigen Peers gibt – außer einem; er muss also mindestens mit einem Knoten verbunden sein, der nicht vom Angreifer kontrolliert wird, um eine eindeutige Identifizierung zu verhindern.

Allerdings ist bedingungslose Sicherheit eine Sicherheit ohne Boden und so gelten drei allgemeine Sicherheitsannahmen, die in keinem Fall gebrochen werden dürfen: der Angreifer darf nicht in der Lage sein, (a) die kryptographischen Annahmen zu brechen oder Nutzung kryptographischer Verfahren/Tools zu verhindern, (b) Endnutzersysteme zu kompromittieren[41] und (c) flächendeckende Netzwerkkommunikation zu verhindern.

Offenes P2P-Modell

Das Angreifermodell ist zudem in einer zweiten Hinsicht anspruchsvoll, insofern eine Synthese mit einem offenen Systemmodell angestrebt wird. In einem offenen Systemmodell gibt es keine Zugangskontrollen, so dass jeder Peer mittels JOIN- oder LEAVE-Operationen ein- oder austreten kann, wie er möchte. Die Informa-

[40] Grothoff (2013); Bennett und Grothoff (2003).

[41] Warum diese Annahme sinnvoll ist, hat Rainer Rehak (2011) in einer ausführlichen Analyse der Auswirkungen des Staatstrojaner-Einsatzes untersucht. Beneš (2014) unternimmt den Versuch, durch eine Kombination aus offenem Hardware-Design und freier Software ein System zu konzipieren, das physische Angriffe entdeckt und als Reaktion darauf kryptographische Schlüssel und sensible Informationen sicher löscht.

tionssicherheit des Systems muss also letztlich zweideutig verstanden werden: einerseits die Umsetzung von Privacy als Schutz von personenbezogenen Informationen, andererseits der Schutz eines gemeinnützigen Systems, und zwar so, dass die Netzwerkprotokolle störungsfrei funktionieren.

Dieser Verweis auf die (gesicherte) Offenheit ergänzt einen weiteren bedeutenden Methodenansatz des GNUnet-Projekts, nämlich dem Entwurf von Netzwerkprotokollen nach dem P2P-Modell. Reine P2P-Modelle sind inhärent hierarchielos, demzufolge darf es auch keinen autoritativen Dienst geben, der eine Zugangskontrolle ausübt. Vielmehr müssen Techniken für Protokolle, Algorithmen und Datenstrukturen zusammengebracht werden, *um Daten und Datenverarbeitung zu dezentralisieren*. Ein berühmtes Beispiel für eine solche Technik ist eine Distributed Hash Table. Hierbei handelt es sich um eine Datenstruktur aus Key-Value-Paaren, auf die mit einem Schlüsselwort zugegriffen werden kann und ein Wert zurückgeliefert wird. Dieser Wert kann lokal oder aber über ein Routing-Protokoll erst erreichbar sein. Eine am antiautoritären Wert orientierte Praxis versucht eben solche Techniken zu entwickeln, zusammenzuführen und nutzbar zu machen.

Was uns die Wertvorstellungen und Modelle nur erahnen lassen, werden wir mit den nächsten Schritten tiefer erkunden, indem wir auf das »technische Gerät« näher eingehen. Auf dieser Ebene spielen Ziele und die Orientierung »an der Sache«, also die sachlichen Bedingungen wie z. B. der Stand der Technik oder das soziale Bedürfnis nach einem File-Sharing-System, eine zunehmende Rolle. Diese Ziele lassen sich als Konkretisierungen der Werte im Bezug auf spezifische Sachverhalte oder Problemstellungen auffassen.

3. Das GNUnet-System

Wir müssen uns dem GNUnet-System aufgrund seines Umfangs schrittweise nähern. Der erste Schritt wird sein, eine genetische beziehungsweise historisierende Analyse durchzuführen, die uns ein sinngebendes Bild vor Augen führt, um der anfänglichen Unübersichtlichkeit Herr zu werden. Der zweite Schritt besteht dann darin, die historischen Produkte *im System* zu begreifen. Dazu werde ich, orientiert am Begriff

des GNUnet *als* Internet, die wesentlichen technischen Dienste, Eigenschaften und Funktionen herausstellen.

3.1. Zur Genese der Technik

Die folgende historische Rekonstruktion basiert zum einen auf den gesammelten wissenschaftlichen Veröffentlichungen[42] zum GNUnet-Projekt, zum anderen auf den Dokumenten aus dem GNUnet-Deleveloper-Archiv.[43] Ich habe die historische Entwicklung nach programmatischen und ideellen Gesichtspunkten in drei Phasen geordnet. Sie mögen uns eine Orientierung geben im Bezug auf die Ziele und ihre Ausgestaltung und lassen sich folgendermaßen charakterisieren: Die erste Phase legt ihren technischen Fokus auf die Entwicklung eines anonymen und dezentralen File-Sharing-Systems; dieses System wird in der zweiten Phase nunmehr eines von vielen zukünftigen Internetdiensten darstellen, die sich in einem umfassenderen System mit der Bezeichung »P2P-Framework« eingliedern werden; schließlich ist die dritte Phase von der Vision und der Anstrengung geprägt, das GNUnet zu einer Alternative für das realexistierende Internet zu heben. Wo nötig, werde ich auf besondere technische Details eingehen.

File-Sharing

In den 2000er Jahren wurde durch das Phänomen Napster das rechtliche Problem des File-Sharing der breiten Öffentlichkeit bekannt – einschließlich der Machtfülle der Musik-Industrie und ihrer Vasallen. Für die Softwareentwickler ergab sich unter anderem aus diesem rechtlichen und politischen Problem die Konsequenz, die Idee einer technisch realisierten Anonymisierung und Zensurresistenz voranzutreiben.

In diesem Kontexte nimmt die Geschichte des GNUnet-Projekts ihren Anfang mit der Erstveröffentlichung von Bennett, Grothoff, Horozov, Patrascu und Stef (2002a) an der Fakultät für »Computer Science« der Purdue Universität und dem

[42] Im Internet: https://gnunet.org/bibliography?f[keyword]=2, Stand 1.9.2014.

[43] Im Internet: https://lists.gnu.org/archive/html/gnunet-developers/. Stand 1.9.2014.

ersten Release des GNUnet-Quellcodes in der Version 0.0.0.[44] Diese Schrift markiert gewissermaßen das Programm für die erste Phase von 2001 bis 2007/2008, in dem hauptsächlich ein anonymes und verteiltes File-Sharing-System angestrebt wird, und zwar basierend auf dem P2P-Ansatz. Damals war dieser Ansatz gegenüber dem Mix-Cascade-Ansatz (vergleichbar mit einer invariablen Kette von TOR-Routern) in der PET-Gemeinschaft hoch umstritten und kulminierte in einer Podiumsdiskussion auf dem PET-Workshop 2004, an dem Claudia Díaz, George Danezis, Christian Grothoff, Andreas Pfitzmann und Paul Syverson teilnahmen.[45] Die von Chaum (1981) herrührende Idee der Mixe als zentraler Baustein für anonyme Kommunikation war ausschlaggebend, nur wie sollte man diese für leistungsfähige Kommunikationsnetzwerke organisieren? Die Wertentscheidung fiel für das GNUnet-Projekt zugunsten des P2P-Ansatzes aus, dabei hatten sie bereits eine Idee ausgearbeitet, um Anonymität effizient und nahezu unabhängig vom Rest des Netzwerkes zu erlangen. Zwar war Anonymität das vornehmliche Ziel, aber es ging doch um mehr: nämlich Anonymität für den Nutzer, Abstreitbarkeit für die Teilnehmer und Dezentralisierung ohne jegliche Autorität für das gemeinnützige System zu erreichen.[46]

Mit diesem Ziel im Hinterkopf produzierte das GNUnet-Projekt vereinzelte Schriften, welche die wesentliche Systemaspekte aufschlüsseln, die in das entwickelte System mündeten. Ein näherer Blick soll uns dabei helfen, einen heute wichtigen Dienst des GNUnet-Systems zu verstehen:

Kommunikationsmodell

Unter anderem wird bei Grothoff, Patrascu, Bennett, Stef und Horozov (2002, S. 5 ff.) das Kommunikationsmodell für ein offenes dezentrales P2P-Netzwerk beschrieben, offen für jeden und dezentral ohne jegliche Autorität. Unter einem solchen Kommunikationsmodell ergibt sich jedoch das schwierige Problem, dass die partizipierenden Knoten grundsätzlich nicht vertrauenswürdig sind. Die hier gefundene Lösung ist daher, dass jeder Knoten seine Kommunikationspartner anhand ihres beobachteten Verhaltens bewertet und mit entsprechenden Sicherheitsmechanismen reagiert, einerseits, und andererseits für seine eigenen Ressourcen selbst verantwortlich ist. Erst durch dieses Prinzip des »lokalen Wissens« erscheint es machbar,

[44] Weitere Ergänzungen finden sich in dem Whitepaper von Grothoff et al. (2002) des selben Jahres.
[45] Díaz et al. (2004).
[46] Bennett et al. (2002b, S. 1).

ein global skalierbares und offenes Netz zu konstruieren beziehungsweise entstehen zu lassen.

Kodierungsschema

Der nächste Systemaspekt ist das File-Sharing-Kodierungsschema »Encoding for Censorship-Resistant Sharing« (ECRS) mit seinem Grundoperationen zum Einfügen (Kodieren), Verteilen und Wiederfinden von Dateien und Verzeichnissen mittels Schlüsselwörter. Die Entwurfsziele dieses Kodierungsschemas sind Zensurresistenz, Abstreitbarkeit und Dezentralität. Grothoff, Bennett und Lindgren (2003) greifen dafür auf das Konzept der *Content Hash Keys* (CHK) zurück, um Datenblöcke mit dem eigenen Hash-Wert des Klartextes zu verschlüsseln und über einen zweiten Hash-Wert des daraus entstandenen Kryptogramms adressierbar zu machen. Dieser zweite Hash-Wert ist also der Query-Hash, über den das Kryptogramm adressiert und heruntergeladen werden kann. Anstatt aber eine ganze Datei auf diese Weise (wie im Freenet) zu kodieren und im Netz abzulegen, wird die Datei zuvor in gleich große 32 Kilobyte-Blöcke aufgeteilt, mit CHKs kodiert und anschließend eine *Merkle-Baumstruktur* mit zusätzlichen Metainformationsblöcken generiert. Diese Blöcke lassen sich gut verteilen und replizieren, wodurch effizientes Load Balancing und Swarming mit Blick auf die Dezentralisierung möglich wird. Die Abstreitbarkeit des Besitzes oder der Autorenschaft von Inhalten wird durch das Kodierungsschema ebenfalls gefördert, da der Vermittler oder Hoster eines einzelnen verschlüsselten Blocks plausibel behaupten kann, dass ihm das Zusammensetzen und Entschlüsseln für die Kenntnis des Inhaltes nicht möglich ist. *Information Hiding* bezeichnet den allgemeinen Ansatz, um zensurresistente Systeme zu entwickeln. Im Kodierungsschema wird dies durch die Verschlüsselung und Verteilung der Inhalte sowie der kryptographischen Verschleierung der Queries erreicht.

Anonymität

Das »GNUnet Anonymity Protocol« ist bei Bennett und Grothoff (2003) beschrieben. Das GNUnet propagiert eine neue Perspektive auf die praktisch umgesetzte Idee von Anonymität: Jeder Peer führt selbst die Funktion eines Mixes durch. Ein einzelner Peer benutzt die Nachrichten, die er von anderen Peers bekommen hat, um seine eigenen Anfragen zu verstecken. Damit schützt diese Technik nicht den ursprünglichen Sender oder Empfänger von Nachrichten, sondern den vermittelnden Peer selbst. Dies erschwert dem Angreifer, einen Zusammenhang zwischen dem Initiator und seiner Aktivität herzustellen.

Ökonomisches Modell

Der letzte zentrale Systemaspekt betrifft das bekannte Problem der Ressourcen-Allokation in P2P-Netzwerken mit nicht-vertrauenswürdigen Peers. Als informationstechnische Ressourcen gelten beispielsweise Bandbreite oder Rechenleistung. Grothoff (2003) hat als Antwort ein ökonomisches Modell entworfen, das zwei Anforderungen erfüllen soll: Erstens, Teilnehmer für ihren Beitrag mit besseren Netzwerkdiensten würdigen, und zweitens, einen Schutz vor Angriffen (z. B. Flooding, Freeloading oder Übernutzung) gewährleisten. Ressourcen-Überschuss in Bandbreite und Rechenleistung ist die Quelle für Vertrauen in unbekannte Peers.[47] Ist ein Knoten im Leerlauf, kann er Anfragen beantworten und für diese Leistung Vertrauen bei den anderen gewinnen. Werden Anfragen gestellt, reduziert dies den zahlenmäßigen Wert des Vertrauens; Vertrauen kann also verlustig gehen, niemals jedoch in Misstrauen (negative Werte) übergehen. Es wird auf Basis des lokalen Wissens von jedem Peer autonom im Kommunikationsvorgang mit anderen entwickelt.

Die Nutzung von Netzwerkressourcen durch bösartiges oder fehlerhaftes Verhalten wird durch den Einsatz dieses ökonomischen Modells ebenfalls erfasst: zu viele Anfragen ohne entsprechendes Vertrauen beziehungsweise genügend Ressourcen-Überschuss werden schlicht nicht beantwortet – ohne dabei andere gutwillige und vertrauenswürdige Peers unbeantwortet zu lassen.

Network-Overlaying

Das anfängliche System war zum Zeitpunkt seiner Erstveröffentlichung bereits äußerst komplex und anspruchsvoll. Ins Blickfeld gerieten weitere Hindernisse für P2P-Kommunikation, die überwunden werden mussten. Früh diagnostizieren Ferreira, Grothoff und Ruth (2003), dass das Kommunikationsmodell des Internet-Protokolls zunehmend durch »politische und technische Veränderungen« die Eigenschaften von P2P-Kommunikation zu verlieren begann und sich als direkte Unterlage nicht eignete. Als Antwort darauf entwickelten sie eine Abstraktionsschicht, welche die Unzulänglichkeiten des darunterliegenden Internets wie zum Beispiel Firewalls, Network Adress Translation (NAT) oder dynamische IP-Adressvergaben zu bewältigen versuchte und gleichzeitig die Möglichkeit bot, auf verschiedenen Transport-Protokollen wie zum Beispiel UDP, HTTP, HTTPs oder SMTP aufzuset-

[47] Bennett et al. (2002a, S. 12).

zen.

Sicheres, vertrauensbasiertes Peer-to-Peer-Framework

Es scheint, dass sich in den Jahren 2007/08 ein bemerkenswerter Fortschritt abzeichnet. Während der technische Fokus noch zuvor auf dem anonymen und verteilten File-Sharing lag, wird nun die Erforschung und Entwicklung eines »sicheren P2P-Frameworks« programmatisch festgelegt und vorangetrieben. Mit dem Release 0.8.x[48] verliert das Ziel der Anonymität seine herausragende Rolle und das File-Sharing-System wird zu einer On-Top-Anwendung des Frameworks neben anderen.

Im Jahr 2009 gründet Christian Grothoff als Projektleiter die »Free Secure Network System Group« und institutionalisiert die wissenschaftliche Arbeit innerhalb des Informatik-Instituts der Technischen Universität München (TUM). Zu den Schwerpunkten gehört der Entwurf und die Implementierung von sicheren Netzwerkprotokollen (im Bereich von P2P-Netzen), Software-Engineering-Tools (speziell statische Analysetools) und Portabilitäts- und Regressionsanalysetools und schließlich die Weiterentwicklung des GNUnets.[49] Viele Forschungsergebnisse der Gruppe haben einen allgemein anwendbaren Charakter, doch ihre konkrete Ausgestaltung, Funktionsweise, Wirkungsweise und Optimierung wird im GNUnet-Framework erprobt.

Die meines Erachtens wichtigsten Entwicklungen in dieser Phase betreffen den Transport (als unterste Schicht/Fundament des GNUnets), das GNUnet-Framework (GNUnet-Core und GNUnet-Dienste) und neue Experimentiertechniken, um P2P-Netze wissenschaftlich zu evaluieren.

Transport

Ein Problem, das sich für nahezu alle P2P-Overlay-Netzwerke stellte, ist die Frage, wie sich der große Teil von Peers, die hinter einem NAT-System liegen, in das P2P-Netz integrieren lässt – mit der zusätzlichen Schwierigkeit, keine weiteren dedizierten Server einzusetzen (Problem des Single-Point-of-Failure). Dieses Pro-

[48] Auch die Codebasis – ein nicht zu unterschlagender Umstand in einer Disziplin, in der lesbarer und gut strukturierter Code die produktive Entwicklung aufrecht erhält – hat sich in ihrer Architektur stark verändert. Einschneidend war hier der Übergang vom Multi-Thread- zum Multi-Process-Modell.

[49] Grothoff (2011).

blem betrifft den Transport, der dafür zuständig ist, eine allgemeine Konnektivität zwischen Peers herzustellen. Mit dem »Autonomous NAT-traversal«-Ansatz von Müller et al. (2010) existiert nun ein Vefahren, mit dem ein Peer mit einem anderen Peer, der hinter einem NAT-System verborgen liegt, eine Verbindung herstellen kann. Neben diesem »NAT-zu-Peer«-Ansatz ist jedoch weitere Forschung nötig, um auch »NAT-zu-NAT« zu ermöglichen.

Auf der gleichen Ebene wurde auch ein Mechanismus für die Selektion des besten Transport-Protokolls – also HTTP, TCP, UDP, Distance Vector (eine Form von Onion-Routing), WLAN, Bluetooth u. Ä. – erforscht und entwickelt. Die wesentliche Idee daran ist, Punkt-zu-Punkt-Verbindungen mit verschiedenen physikalischen Verbindungen oder Verbindungsprotokollen herzustellen und diesen Fakt gegenüber höheren Layern (z. B. dem darüberliegenden GNUnet-Core) zu verstecken.[50] Eine weitere Schwierigkeit für P2P-Netzwerke stellen unstrukturierte Netze mit spärlich verbundene Peers dar, da die allgemeine Annahme der meisten P2P-Ansätze stets *universelle Konnektivität* war. Beispielsweise ist in einem GNUnet-Maschennetzwerk ohne IP-Routing mit mindestens zwei Hops zwischen zwei Knoten eine solche universelle Konnektivität nicht gegeben. Das Distance-Vector-Routing (als GNUnet-Dienst) erfüllt im wesentlichen diese Aufgabe und findet effizient lokale Routen bis zu drei Hops.

GNUnet-Framework

Einige der neu hinzugekommenen GNUnet-Dienste und -Funktionen neben der File-Sharing-Anwendung sind der MESH-Dienst für Ende-zu-Ende-Kommunikation, der VPN- und Protokoll-Translation-Support,[51] eine randomisierte Distributed Hash Table (DHT) als verteilter Informationssspeicher für Key-Value-Paare und, darauf basierend, der Routing-Algorithmus R^{5}N (Kurzform für »Randomized Recursive Routing for Restricted Route Networks«). Zusammengenommen ergeben sie das GNUnet-Framework.

Die virtuelle Netzwerkschnittstellen (zuständig für den VPN/PT-Support) hat drei Funktionen: Erstens lässt sich IP-Verkehr über das VPN zu einem Exit-Node

[50] Genauer gesagt geht der GNUnet-Core von einer universellen Konnektivität aus; diese wird vom Transport so gut wie möglich zur Verfügung gestellt. Siehe dazu die Studie von Wachs (2015).

[51] Im Internet: `https://gnunet.org/gnunet090`, Stand: 3.11.15. Der VPN/PT-Dienst basierte damals auf dem Vorläufer von CADET, das damals noch MESH hieß.

tunneln, von wo er dann weitergeleitet wird ins Internet, zweitens ist eine Protokollübersetzung nach IPv4 und IPv6 aus dem GNUnet heraus möglich und drittens lässt sich eine Verbindung zu »internen« GNUnet-Diensten (ähnlich dem Tor-Hidden-Service) herstellen.

Beim Design des DHT-Dienstes kam es darauf an, den Anforderungen der Sicherheit und Skalierbarkeit gerecht zu werden. Unter anderem wurden dafür teilrandomisierte Put- und Get-Operation – als die beiden wesentlichen Operationen einer DHT – entwickelt. GNUnet-Peers in einem IP-Netz führen das verteilte Routing über eine DHT aus.

Der R^{5}N-Algorithmus entstand aus dem »Studium und der Verbesserung von sicheren, dezentralen und robusten Routing-Algorithmen für offene Netzwerke, einschließlich Ad-Hoc- und P2P-Overlay-Netzwerken. Zu seinen Hauptzielen gehören die Offenheit, Effizienz, Skalierbarkeit und Widerstandsfähigkeit gegen verschiedene Angriffe.«[52] R^{5}N-Routing verbindet also das verteilte Routing in IP-Netzen über DHT und das Routing in Multi-Hop-Nachbarschaften über Distance-Vector-Routing.

Zuletzt sei noch auf die Schrift von Evans und Grothoff (2011) hingewiesen, in der sie ein skalierbares Framework zur Evaluierung von P2P-Protokollen einführen. Argumentiert wird, dass eine Emulation ein besseres Modell als eine Simulation für Experimente mit P2P-Protokollen ist, da unter anderem der tatsächliche Code ausgeführt wird. Ein großer Vorteil sei zudem, dass man mit Implementationen in groß angelegten Experimenten experimentieren könne, ohne dass die Nutzer davon betroffen wären. Für die wissenschaftliche Untersuchung und Weiterentwicklung stellt dieses Framework ein großes Hilfsmittel dar.

Experimentiertechnik

Der Weg zum neuen Internet

Ich nehme nun die Schrift von Grothoff et al. (2014) mit dem Titel »The Internet is Broken: Idealistic Ideas for Building a ~~NEW~~GNU Network« zur Abgrenzung für den letzten und aktuellen historischen Abschnitt (beginnt 2013/14) in der Genese des GNUnet-Projekts. Die Vision einer alternativen Internet-Architektur ist nicht erst

[52] Frei übersetzt nach Evans (2011, Abstract).

in dieser Schrift zum Vorschein getreten, dennoch wird hier in einer besonderen Weise die Vorstellung artikuliert, das GNUnet-System in seiner bisherigen Fassung zum Kandidaten eines solchen Unterfangens zu erklären.

Zwei Arbeiten scheinen mir hier relevant, da sie zusammen mit den älteren Komponenten des GNUnet-Systems die Homologie zum Internet begründen: das alternative Namesystem GNS[53] und das sichere Transport-Protokoll CADET[54] als Alternative zur Transport Layer Security (TLS) über TCP.

Im einzelnen handelt es sich beim GNS um ein dezentrales, zensurresistentes Namesystem mit sogenannter Query-Privacy, also Vertraulichkeit der GNS-Anfrage, und einer sicheren Namensauflösung. Dabei wurde darauf geachtet, dass GNS interoperabel ist mit bestehenden Namesystemen wie DNS oder .onion-Adressen des Tor-Netzwerks. Bemerkenswert ist die Doppelfunktion, denn das GNS eignet sich auch als dezentrale und sichere Public-Key-Infrastruktur (PKI). Damit stellt das GNUnet-Projekt auch eine Alternative zur bestehenden X.509-CA-PKI in Aussicht.

Bei CADET handelt es sich um ein sicheres und dezentrales Transport-Protokoll, dass von seiner Funktionalität her mit TCP/IP vergleichbar ist, allerdings eine Vielzahl weiterer Eigenschaften besitzt. Entworfen wurde es mit dem Ziel, dass ein Knoten in unstrukturierten Netzen (z. B. Ad-hoc- oder P2P-Netze) vertraulich mit einem anderen Knoten kommunizieren und authentisierte Daten austauschen kann. Redundante Routen sorgen für eine höhere Zuverlässigkeit und der Routing-Algorithmus R^5N wird für eine sichere Konnektivität in Anwesenheit eines aktiven Angreifers verwendet.

Mit »SecuShare« hat Toth (2013) zusammen mit v. Loesch und Grothoff erste Anwendung für soziale Netzwerke entwickelt, welche auf dem bisher genannten Algorithmen des GNUnet-Systems und dem effizienten, textbasierten Multicast-Protokoll PSYC aufbaut. Es modelliert soziale Netzwerke als verteilte soziale Graphen, in denen die Teilnehmer (Menschen, Gruppen, Maschinen) eines sozialen Graphens wechselseitig kryptographisch authentisiert sind, aber deren Kommuni-

[53] GNS: »GNUnet Name System«, in Anlehnung an das Domain Name System. Siehe Wachs et al. (2014). Die Arbeiten am GNS hatten bereits 2012/13 begonnen, damals bekannt unter dem Namen »GNU Alternative Domain System« (GADS).

[54] CADET: »Confidential Ad-hoc Decentralized End-to-End Transport«. Siehe Polot und Grothoff (2014).

kation und Metadaten gegenüber nicht teilnehmenden Entitäten kryptographisch geschützt sind.[55]

3.2. Das System: Dienste, Eigenschaften und Funktionen

Wir haben bis hierhin eine historische Rekonstruktion durchgeführt, um die Entstehungsbedingungen, Zielstellungen und Probleme ausgewählter GNUnet-Arbeiten in den Blick zu bekommen. Das große Ganze steht nun bevor: das GNUnet-System *als* vernetzbares Host-System. Oder, um es von seiner strukturellen Seite zu betrachten, das GNUnet *als* Internet. Mit dem Bezug auf das Internet ist auch ein Anspruch verbunden, dem das GNUnet-Projekt gerecht zu werden versucht. Wichtig ist dabei zu erkennen, dass mit dem Begriff des Internet zwar auch die Vorstellung einer lebendigen soziale Sphäre oder das breite Angebot an bereits bestehenden Internet-Anwendungen assoziiert sein kann (die das GNUnet zur Zeit nicht aufbieten kann). Vielmehr scheint mir aber sein Begriff in der *sozialen Aufgabe/Funktion* begründet, einen globalen und schnellen Informationsaustausch über digital vernetzte Medien und lokale Netze zu ermöglichen.[56]

Für den weiteren Verlauf meiner Arbeit möchte ich aus der reichhaltigen Fülle der verwendbaren Tools, Algorithmen und Diensten (über 30 an der Zahl), die das GNUnet-Framework anbietet, einige meines Erachtens besondere Softwarekomponenten in den Fokus nehmen, deren Relevanz sich sich aus der Homologie zum Internet ergibt. Die Systemeigenschaften und -funktionen dieser Komponenten sollen dazu kurz beschrieben werden.

[55] Im Internet: `http://about.psyc.eu/`, Stand: 24.01.2016.

[56] Erst aus diesem begrifflichen Bezug ist eine normative Bewertung oder Kritik überhaupt möglich, wie ich sie in meiner Arbeit durchführe. Der Begriff einer Sache ist nämlich gleichzeitig normativ wie deskriptiv, er gibt Maßstäbe der Verwirklichung vor, die aber potentiell bereits in der Sache liegen. Das GNUnet kann damit zwar defizitär sein verglichen mit dem realexistierenden Internet und in genau diesem Sinne »seinem Begriff nicht entsprechen«. Aber es wäre abwegig, vom GNUnet begrifflich als LAN-Technik zu sprechen.

Informationssicherheit als Systemeigenschaft

Beginnen wir mit der Informationssicherheit, die ja schließlich eine herausragende Bedeutung im GNUnet-Projekt hat, lassen sich die folgenden kryptographischen Primitiven dokumentieren.

Perfect Forward Secrecy[57] (PFS) ist Stand der Wissenschaft und wird auch vom GNUnet-Projekt in verschiedenen Diensten eingesetzt. Für die Public-Key-Kryptographie ist das GNUnet-System 2013 vom RSA-System auf das schnelle und noch nicht »kompromittierte« Curve25519-System von Bernstein (2006) umgestellt worden. Dieses ist ein Baustein für den Signatur-Algorithmus Ed25519 von Bernstein, Duif, Lange, Schwabe und Yang (2012), der für die Authentifizierung benutzt wird. Für den authentifizierten Schlüsselaustausch wird das Protokoll ECDHE verwendet, während AES-256 und Twofish-256 für die Verschlüsselung zur Gewährleistung der Vertraulichkeit verwendet wird. Die (authentifizierte) Integrität wird mittels SHA-512 (»encrypt-than-MAC«) gewährleistet.

Die genannten kryptographischen Primitiven werden beispielsweise für die Link-Sicherheit zwischen den einzelnen nachbarschaftlichen Peers verwendet, für den Ende-zu-Ende-Transport zwischen zwei entfernten Peers oder das GNUnet Name System, mit Hilfe dessen zusätzliche kryptographische Identitäten hergestellt werden können, die dann mit weiteren Daten (zum Beispiel einer Webseite) verknüpft werden können.

Zuverlässigkeit als Systemeigenschaft

Die Sicherheit im Sinne der Zuverlässigkeit gegenüber Peer-Fluktuationen (Churn), byzantinischen Fehlern oder Ressourcen-Übernutzung (z. B. Freeloading) sind auf unterschiedliche Weise innerhalb des P2P-Modells der einzelnen Systemdienste umgesetzt, ein Beispiel ist das in Abschnitt 3.1 beschriebene ökonomische Modell des File-Sharing-Dienstes.

[57] Zur Definition von Diffie et al. (1992, S. 7): »An authenticated key exchange protocol provides perfect forward secrecy if disclosure of long-term secret keying material does not compromise the secrecy of the exchanged keys from earlier runs. The property of perfect forward secrecy does not apply to authentication without key exchange.«

Auf der Entwicklungsebene hinsichtlich der Codebasis wurden seit der Version 0.9.0 unterschiedliche tiefgreifende Maßnahmen unternommen, um die Zuverlässigkeit der Software zu verbessern.[58] Hervorzuheben ist die Transformation der Architektur und Prozessorganisation hin zum Multi-Process-Model mit einem Supervisor-Prozess, der abgestürzte Dienste automatisch neustartet. Dadurch können Fehler isoliert werden, der Code besser getestet und gewartet werden. Daneben wurden die Testmechanismen umfangreich reorganisiert, um einzelnen Module für bis zu 90.000 Peers zu testen.[59]

Systemdienste als Komponenten

Die Abbildung 1 zeigt die ausgewählten Dienste des GNUnet-System und stellt sie vergleichbaren Internetdiensten gegenüber, ausgerichtet an zwei typischen Kommunikationsmodellen (P2P-Systemmodell und Netzwerkmodell, vereinfacht nach ISO). Ich erläutere die Dienste von unten nach oben entlang des P2P-System-Modells (siehe Abbildung 1).

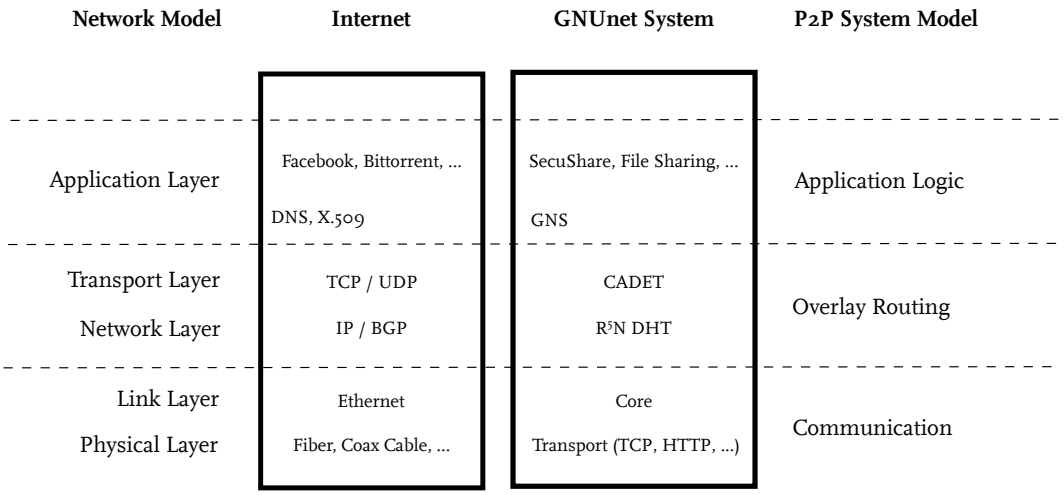


Abbildung 1: Vision des GNUnet-Projekts: Eine vereinfachte Gegenüberstellung des Netzwerkstacks des realexistierenden Internets und des GNUnets.

[58] Im Internet: https://gnunet.org/gnunet090, Stand: 24.1.2015.
[59] Totakura (2013).

Communication Der GNUnet-Transport ist vergleichbar mit der physikalischen Schichten des Internets. Hardware ermöglicht die Kommunikation zwischen physisch verbundenen Rechnern durch Hin- und Rückübersetzung von physikalischen Signalen und Bits. Der GNUnet-Transport stellt Netzwerkkonnektivität zwischen Peers her, um die Bedingung der Möglichkeit für Kommunikation zwischen verbundenen Rechnern zu schaffen. Diese Funktion potenziert sich durch Plugins für WLAN, Bluetooth, TCP, UDP, HTTP(s) und SMTP, mit denen sich eine große Masse weiterer Peers erreichen lässt, auch Overlay-Netzwerk genannt. Diese (teilweise unverschlüsselten) Links sind der »Rohstoff« für das P2P-Netz.

GNUnet-Core ist vergleichbar mit dem Ethernet, da er funktional gesehen logische Links mit besonderen Eigenschaften zwischen den erreichbaren Peers herstellt. Diese Links sind mittels OTR verschlüsselt und authentisiert. Ferner adressiert GNUnet-Core Peers nicht über MAC- oder IP-Adressen, sondern über ECC-Public-Keys,[60] die als Identitäten fungieren und gleichzeitig für die Authentifizierung verwendet werden. Zusammen mit dem GNUnet-Transport führt es das Peer-Discovery durch, um das P2P-Overlay-Netzwerk zu bilden. Dazu werden u. a. sogenannte HELLO-Nachrichten per Broadcast an andere Peers verschickt, die die Peer-Identität und die signierte Netzwerkadresse beinhalten. Netzwerkadressen werden mittels eines Public-Keys signiert, um die Peer-Identität an eine Netzwerkadresse zu binden und damit gegen Spoofing und dergleichen abzusichern.

Overlay Network R^{5}N-DHT ist als Routing-Algorithmus vergleichbar mit IP (RIP, OSPF) bzw. BGP.[61] Im Gegensatz zu den Punkt-zu-Punkt-Verbindungen von GNUnet-Core ist seine Funktion also Multi-Hop-Routen mittels »Source-Routing«[62]

[60] Dies sind Schlüssel, die mittels Elliptischer-Kurven-Kryptographie wie z. B. Curve25519 erstellt wurden.

[61] Border Gateway Protocol: Es wird verwendet, um zwischen den verschiedenen IP-Netzen, auch bekannt als Autonome Systeme, zu routen.

[62] Source-Routing bezeichnet im Allgemeinen ein Verfahren, bei dem ein Knoten in einem zusammenhängenden Graphen einen Route-Request auslöst und an verschiedene Knoten im Graph sendet. Jeder Knoten, der das Route-Request weiterleitet, trägt seine Adresse in den Route-Request als zusätzliche Information ein. Der Route-Request wird von den Knoten solange weitergeben, bis ein Knoten sich selbst als Ziel identifiziert, sich ebenfalls einträgt und auf den Request antwortet, indem er die Liste zurücksendet.

zu finden. Aufgrund der Randomisierung gibt R^{5}N-DHT unterschiedliche Routen aus, wobei eine Route als Liste von Peers zurückgegeben wird. Dies macht ihn u. a. gegenüber aktiven Angreifern robust. Die Routing-Tabelle selbst ist eine DHT.

GNUnet-CADET ist vergleichbar mit TCP/UDP, seine Funktion ist es, den Verkehr zwischen zwei Peers mittels OTR von Ende zu Ende abzusichern (authentisierte Verschlüsselung) und zu kontrollieren (z. B. optional durch Congestion Control oder zuverlässige Packet-Vermittlung). Zudem besitzt eine Verbindung die Eigenschaft, 3-fach redundant zu sein, d. h. drei unterschiedliche Routen gleichzeitig zur Verfügung zu haben. Der Zweck ist mehr Zuverlässigkeit und Leistung zu erreichen.

Application Logic Auf der Applikationsebene befindet sich das GNU-Name-System, das wiederum vergleichbar ist mit dem Domain-Name-System. Seine Funktion besteht darin, Namen sicher und dezentral in Netzwerkadressen aufzulösen. Das Namesystem ist einem bekannten »Petname«-System[63] nachempfunden worden, weshalb die Namen die besondere Eigenschaft besitzen, sicher und einprägsam zu sein, im Gegensatz zu den DNS-Domain-Names, die einprägsam und global sind. Damit die Petnames dennoch global verfügbar sind, wurde das dezentralisierte Konzept der sicheren Zonen-Delegation eingeführt. Eine zusätzliche wichtige Eigenschaft ist die »Query-Privacy«, dabei wird die Namensanfrage selbst mittels Hashing verschlüsselt.

Eine außergewöhnliche Zusatzfunktion ist ihre Verwendung als Public-Key-Infrastruktur (PKI): Ein Name kann in einen Schlüssel aufgelöst werden. Erweitert wurde dies um Subfunktionen, die letztendlich ein Identity-Management ermöglichen.

Der GNUnet-File-Sharing-Dienst wurde bereits in Abschnitt 3.1 eingehender erörtert. Seine Funktion besteht einerseits darin, Dateien anonym und zensurresistent austauschen zu können und andererseits Dateien dezentral als Backup im Netz zu speichern.

Die GNUnet-Anwendung SecuShare ermöglicht den Aufbau sozialer Netzwerke, in denen die sozialen Beziehungen zwischen Menschen, Gruppen und Maschinen durch soziale Graphen modelliert werden. Sein Funktionsumfang beinhaltet pro-

[63] Die Rede ist hier vom SDSI/SPKI-Design von Rivest und Lampson (1996).

grammierbare Chaträume mit Präsenz-Nachrichten, Ereignis-Benachrichtigungen, News- und Friendcasting, Telefonie- und Videokommunikation. SecuShare hängt von den GNUnet-Diensten GNS, CADET und Core ab.

3.3. Zwischenfazit

An dieser Stelle ist die Analyse des GNUnet hinreichend abgeschlossen, um die Frage zu beantworten, was das GNUnet eigentlich ist. Zu seinem technologischen Begriff kommen wir, indem wir die Betrachtungen zum GNUnet-Projekt als offener Organisation, die Betrachtungen zu den philosophischen und politischen Wertvorstellungen und zuletzt das technische System als offener Plattform für zukünftige Internetkommunikation zusammenführen. *Das GNUnet ist damit eine dezentrale sicherheitsorientierte P2P-Netzwerktechnologie mit einem ausgesprochen ethisch-politischen Charakter.*

Mit diesen Begriff können wir nun einen Schritt weiter gehen und den folgenden sozialtheoretisch untersetzte Gedanken formulieren, dass nämlich das GNUnet eine *herrschaftsfreie* P2P-Netzwerktechnologie ist. So gesehen stellen sich dann nämlich die folgenden Fragen: Welche Veränderungen sind eigentlich im Sozialen zu erwarten? Und lassen sich die digitalen Kommunikationsformen gerade so verändern, dass wir das offene und akute Problem informationeller Macht – wie ich sie oben umrissen habe – auf diesem Weg in den Griff bekommen? Darum soll es im nächsten Teil gehen.

Teil III.
Soziale Wirkung

»There are many fights more important than the fight over how the internet is regulated. Equity in race, gender, sexual preference; the widening wealth gap; the climate crisis – each one far more important than the fight over the rules for the net. Except for one thing: the internet is how every one of these fights will be won or lost. Without a free, fair and open internet, proponents of urgent struggles for justice will be outmaneuvered and outpaced by their political opponents, by the power-brokers and reactionaries of the status quo. The internet isn't the most important fight we have; but it's the most foundational.« – Cory Doctorow

Technologien mit einem emanzipatorischen Anspruch richten sich, vereinfacht gesprochen, auf die Veränderung sozialer Verhältnisse, und zwar dort, wo sie gemessen an den Idealen der Freiheit, Gleichheit, Autonomie oder Ähnlichem kritikwürdig oder verbesserungsbedürftig erscheinen. Beim genaueren Hinsehen mag es jedoch schwer fallen, bei einer so komplexen Technologie wie dem GNUnet, die Folgen angemessen zu erfassen und zu bewerten. Die Gefahr dabei ist, um es mit den Worten Joseph Weizenbaums zu sagen, dass die Folgen einer Technik weniger von den Eigenschaften abhängen, die sie tatsächlich besitzt, sondern die ihr von einem Publikum – angefangen bei der Presse bis zum dilettierenden Informatiker oder Internet-Aktivisten – zugeschrieben und vom Laien übernommen werden. Anti-Viren-Software ist dafür vielleicht ein anschauliches Beispiel: Es zeigt, wie Millionen von Menschen auf ihre (von Informatikern) versprochene Wirkung vertrauten, ohne zu ahnen, dass sie damit einer ganzen Malware-Industrie Tür und Tor zu ihren persönlichen Geräten öffneten, indem vermeintliche Anti-Viren-Software verteilt und installiert wurde.[64] Um dies zu vermeiden wird es also nötig sein, das Verhältnis zwischen dem (intellektuell durchdrungenen) GNUnet und dem Sozialen zu untersuchen. Ausgerichtet an der Fragestellung der Informationsmacht, die zusammen mit der Freiheitsidee zum thematischen Bezugspunkt des GNUnet-Projekts gehört, werde ich im ersten Abschnitt zunächst einen soziologisch begründeten Begriff der Informationsmacht einführen und anschließend im zweiten Abschnitt versuchen, eine Folgenabschätzung zu treffen. In Teil IV soll diese technikanalytisch bezogene Folgenabschätzung über eine Gegenüberstellung mit dem gesellschaftsanalytischen Ansatz des Datenschutzprojektes stärkere Konturen erhalten.

1. Was ist Informationsmacht?

1.1. Begriffsanalyse

Um diese Frage zu beantworten, werde ich zunächst einmal analytisch die beiden Begriffe Information und Macht klären. Information ist von Natur aus bedeu-

[64] Siehe dazu im Internet: https://firstlook.org/theintercept/2015/06/22/nsa-gchq-targeted-kaspersky/, Stand: 24.6.15.

tungsvielfältig, je nach Disziplin unterschiedlich aufgefasst und verwendet. Ein für Informatik besonders aussichtsreicher Informationsbegriff für das hier behandelte Thema der Informationsmacht liefert Wilhelm Steinmüller, der durch Jörg Pohle (2014) eine Reaktualisierung erfahren hat. Information ist hiernach immer ein Abbild oder Modell eines bestimmten Ausschnitts der »Wirklichkeit«, zugeschnitten durch die Interpretation,[65] die Perspektive und den Zweck desjenigen, der die Information erhebt. »Es handelt sich um den Informationsbegriff der Semiotik mit seinen vier Dimensionen Syntax, Semantik, Pragmatik und Sigmatik.«[66] Betrachten wir vor allem die soziale Wirklichkeit, dann wird »mit Syntax dabei die konkrete, meist zeichenmäßige Repräsentation, mit Semantik die Bedeutung und mithin der Kontext, mit Pragmatik der Zweck und mit Sigmatik der Verweis auf die betroffene Person bezeichnet [...].«[67] Ich meine, wir können diesen starken Personenbezug etwas auflockern zugunsten eines allgemeineren Bezugs auf beliebige soziale Akteure (Mensch, Gruppe, Organisation, etc.), denn um sie geht es in einer gesellschaftstheoretischen Betrachtung. Anzumerken wäre noch, dass ein solcher Informationsbegriff ohne die Idee von Information als Eigentum auskommt.

Macht man sich diesen Informationsbegriff zu eigen, ist es verständlich, warum die korrekte Information, dass ein bibeltreuer Katholik »Analphabet ist«, einem schriftkundigen Pfarrer die Möglichkeit einräumt, Ablassbriefe an ihn zu verkaufen. Allgemein gesprochen bedeutet dies, dass mit der Kenntnis einer akteuersbezogenen Information bestimmte *zweckmäßige Handlungsmöglichkeiten* verbunden sind, die vorher nicht offenkundig waren und sich damit auf das Verhalten des Betroffenen nachteilig auswirken können. Es kann sogar sein, dass der betroffene Akteur sich selbst einschränkt, wenn er weiß, *dass* ein anderer Akteur etwas bestimmtes über ihn weiß.

Machtbegriff

Der andere zu klärende Begriff ist Macht. Dazu leihe ich mir umstandslos den Machtbegriff, wie er in verschiedenen Variationen in der Soziologie[68] verwendet

[65] Der hermeneutische Aspekt der Informatik wurde spätestens von Winograd und Flores (1989) extensiv beleuchtet, die mit ihrer Arbeit eine »hermeneutische Wende« (Coy) in der Informatik einleiteten.

[66] Pohle (2014, S. 49).

[67] Ebd.

[68] Vergleiche zum Beispiel Castells (2009, S. 10).

wird: Macht ist eine relationale Eigenschaft eines sozialen Akteurs gegenüber einem oder mehreren sozialen Akteuren. Zwischen zwei sozialen Akteuren gibt es immer eine gegenseitige Beeinflussung und es kommt darauf an, wessen asymmetrischer Einfluss auf den anderen größer ist, um seine(n) eigenen Interessen/Werte/Willen durchzusetzen. Sie wird ausgeübt durch Zwangsmittel (oder der Möglichkeit ihres Einsatzes) und/oder durch Konstruktion von Bedeutung innerhalb eines disziplinären Diskurses, an denen sich das Handeln von Akteuren orientiert. Als Herrschaft bezeichnet man sodann institutionalisierte Formen der Macht.

Begriff der Informationsmacht

Aufbauend auf den vorherigen Grundbegriffen schlage ich folgenden Begriff der Informationsmacht vor. Informationen über einen sozialen Akteur sind ein Abbild oder Modell eines Ausschnittes der sozialen Wirklichkeit, das eine besondere Beeinflussung der Verhaltensbeziehung zu eben diesen Akteur ermöglicht. Dies impliziert logischerweise eine korrekte Sigmatik, also einen korrekten Bezug zu einem Akteur, andernfalls ergäben sich Verzerrungen der semantischen und pragmatischen Dimension und die Einflussnahme könnte ihr Subjekt verfehlen. Durch die *Verkettung* von Informationen über einen Akteur wird der zweckorientierte Handlungsspielraum des »Informierten« größer. Dabei reicht lediglich eine Information, deren Semantik und Pragmatik den Zwecksetzungen des Informierten »zu Gute kommt«. Darin liegt auch der Grund, warum es kein belanglose Information gibt.[69] Der Wert einer Information bestimmt sich unvorhersehbar aufgrund des Verwerters und seines Verwertungsinteresses. Diese Vorbedingung einer vorhandenen Information muss noch um eine zweite Vorbedingung ergänzt werden, nämlich dass der Einfluss selbst durch nötige Zwangsmittel (z. B. Polizei, Kündigungsandrohung, Einreiseverbote, Kommunikationssperren, Veränderung eines technischen Systems[70] oder Werbung) oder die Selbstdisziplinierung des Betroffenen ausgeübt werden kann. Erst dann lässt sich tatsächlich und empirisch von der Informationmacht eines sozialen Akteurs sprechen.

Schwieriger ist die Konsequenz zu sehen und zu beurteilen, dass selbst anonyme

[69] Vergleiche BVerfG, Urteil v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83, Link: http://tlmd.in/u/88

[70] Man denke zum Beispiel an die Sanktionsmittel von facebook, indem es einfach softwaretechnische Veränderungen durchführt und damit die abhängigen Klienten zu einem neuen Verhalten zwingt.

Informationen, das heißt ohne eine genau definierte sigmatische Dimension (jedoch nach wie vor auf Menschen bezogen), eine statistische Praxis ermöglichen, bei der normierte/standardisierte Akteursprofile produziert werden. Einerseits bieten sie dem Informierten generalisierte Handlungsspielräume, andererseits beinhaltet sie aber die Gefahr, abweichendes Verhalten zu Unrecht zu sanktionieren.

Rolle der Computer

Informationsmacht, wie ich sie hier behandle, ist also Macht, die wesentlich auf der Kenntnis von akteursbezogenen Informationen beruht.[71] Mit der computergestützten Informationserhebung, -speicherung, -verarbeitung, -verwendung und -vermittlung potenziert sich der Faktor Macht, insofern Informations- und Kommunikationssysteme einen effizienteren Umgang mit Informationen ermöglichen.

1.2. Das Doppelgesicht der Macht

Kritisch betrachtet gilt es noch eine Besonderheit bezüglich des Machtbegriffs zu klären, die für diese Arbeit relevant ist: das Doppelgesicht der Macht. Saar (2009, S. 575) hat dies präzise formuliert: »Steht auf der einen Seite ein Verständnis von Macht als Herrschaft, steht auf der anderen ein Konzept von Macht als Konstitution; geht es im einen Fall um Durchsetzung und Unterwerfung von Willen, geht es im anderen um die Entfesselung und Kanalisierung von vielfältigen Kräften.«[72] Dies erklärt beispielsweise die widerstreitenden Positionen gegenüber dem Staat: In den Augen der konservativen Verfassungshüter ist er ein Machtmittel zur Konstituierung sozialer Ordnung und Freiheit, im Rahmen der Handlungslogik des Einzelnen ist die Freiheit letztlich gegen diese Macht gestellt.

1.3. Legitimitätsproblem

Hat man die Effektivität der Macht als solche festgestellt, kann die Frage der Legitimität gestellt werden. Problematisch wird Informationsmacht nämlich, wenn sie missbraucht wird und sozial unerwünschte Folgen zeitigt. Dies kann früher oder

[71] Nicht betrachten werden ich Informationen über Dinge wie Bücher, Autos, Häuser oder Flächen. Aber auch über diese lässt sich Macht auf Individuen und Gesellschaft ausüben. Diesen Aspekt gilt es weiter zu untersuchen. Auch das Zensurproblem als wichtiger Aspekt von Informationsmacht blieb hier aus Mangel an Zeit auf der Strecke.

[72] Ebenfalls auf diesem Verständnis gründend: Castells (2009).

später das Problem der Legitimität von Macht aufwerfen. Das Doppelgesicht der Macht weist darauf hin, dass Macht unter den Machtunterlegenen als rechtens gilt und politisch unterstützt wird, sofern sie konstitutiv für bestimmte Freiheiten ist oder zumindest der Glaube daran besteht. Wird sie dysfunktional oder ihr Zweck nicht mehr erkennbar, begleitet von dem starken subjektiven Empfinden, fremdbestimmt zu sein, kann sie in illegitime Macht umschlagen und eine Reaktion der Machtunterlegenen hervorrufen.

Die eingangs verwendete Problemformulierung einer »aus den Fugen geratene Informationsmacht« lässt sich mit diesen Ausführungen nun als illegitime Macht im Informationsbereich verstehen. Damit soll die negative Diagnose zum Anklang kommen, dass eine *faktische* politische oder gesellschaftliche Ordnung, die an neuralgischen Stellen durch Informations- und Kommunikationstechnologien bedingt ist, sich nicht mehr rational am normativen Maßstab einer Verfassung oder moralischer Prinzipien rechtfertigen lässt. Eine solche Diagnose muss sich aber auch von Alltagsmeinungen abheben und einen ausreichenden Grad der Objektivität bieten, ohne Gefahr zu laufen, sich wiederum einer Paternalismuskritik auszusetzen. Objektivierungen dieser Art über illegitime Informationsmacht finden sich in gesellschaftlichen und wissenschaftlichen Diskursen, die zum Beispiel mit Blick auf widerfahrenes Unrecht danach fragen, ob die Datensammlung von Geheimdiensten legitim ist, ob die von Facebook unternommenen automatisierten Bildanalysen gerechtfertigt sind, ob das Traffic-Shaping eines Internet-Anbieters gegenüber seinem Kunden begründet ist, oder ob die ausgewählten Datenfelder in einer Organisation erforderlich sind. In allen vier Fällen ist der Umgang mit Informationen unter Umständen rechtskonform, aber unter politisch-ethischen Gesichtspunkten problematisch. Das soll heißen, dass sich diese politisch-ethischen Infragestellungen dort ergeben, wo Recht und Gerechtigkeit auseinander fallen oder das Recht an seine Grenzen stößt (zum Beispiel wegen der Vollzugsohnmacht der Staaten).

2. Folgenabschätzung des GNUnets

In welchen als illegitim gekennzeichneten Bereichen können nun Machtverhältnisse durch das GNUnet umgestaltet werden und auf welche Weise würde dies geschehen? Um diese Fragen zu beantworten, werde ich eine grundlegende Unterscheidung vornehmen, die an das herausgestellte duale Wertesystem und die davon quasi-abgeleiteten Modellierungsverfahren und Techniken anschließt. Die These ist, dass mit der Logik des Privaten und der Logik des Antiautoritären zwei Arten von Machtverschiebungen sich als Folge des breit eingesetzten GNUnets einstellen werden, nämlich einmal im Bereich der Informationsverarbeitung (IV) und zum anderen im Bereich der Kommunikationsverarbeitung (KV). Während die Logik des Privaten darauf abzielt, vorwiegend die Kommunikation vertraulich und verkettungssicher zu gestalten und dadurch die traditionell vorteilsbehaftete Kommunikationsverarbeitung durch Dritte zu erschweren, so zielt die Logik des Antiautoritären hauptsächlich auf eine dezentrale Informationsverarbeitung, die ehemals als zentrale Informationsverarbeitung in Organisationen betrieben wurde. Diese analytische Trennung ist auch sachlich in der Gegebenheit begründet, dass Kommunikationsinfrastrukturen und Informationsverarbeitungsstrukturen grundsätzlich andere technische Schwerpunkte haben. Auf der sozialen Ebene betrifft die KV das Machtverhältnis zwischen den legitimen Kommunikanten auf der einen Seite und den Vermittlern und sonstigen Mitspielern auf der anderen Seite. Die IV betrifft das Machtverhältnis zwischen Internet-Service-Providern und ihren Nutzern.

An dieser Stelle könnte aber der Einwand erhoben werden, dass eine sozialtheoretisch bedachte Untersuchung nicht auf der technischen, sondern zunächst auf der sozialen Ebene durchgeführt werden müsse. Auf diesen Einwand werde ich später in Teil IV Abschnitt 2 noch einmal näher eingehen, wenn wir das Verhältnis zweier unterschiedlicher Problemperspektiven selbst problematisieren. Vorerst steht fest, dass das GNUnet als Netzwerktechnologie bereits mehr oder weniger ausgewachsen ist und daher vorrangig die Untersuchung der Folgen in Betracht kommt, die mittels der Analyse der Technik zum Vorschein kommt. Die folgenden beiden Abschnitte dienen der Erläuterung dieser beiden genannten Machtverschiebungen als

Folgenabschätzung.

2.1. Über den Machtverlust im Bezug auf Kommunikationsverarbeitung

Beispiel: Ethernet vs. GNUnet-Core

Die spezifische Veränderung von Machtverhältnissen im Sinne des GNUnet-Projekts lässt sich vielleicht am Besten anhand des Vergleichs zwischen GNUnet-Core[73] und eines Link-Layer-Protokolls wie dem Ethernet erläutern. Ich werde diesbezüglich vor allem die kryptographischen Techniken näher erläutern, die in GNUnet-Core zum Einsatz kommen.

Das Ethernet ist eine gängige und grundlegende Form aktueller Rechnerkommunikation für Wide Aread Networks (WAN) und Local Area Networks (LAN), um zwischen physisch direkt verbundenen Rechner Daten auszutauschen. Dazu bedarf es einmal eines Adressierungsschemas – die sogenannten MAC-Adressen – und eines Protokolls, das einen geordneten Datenaustausch regelt. Beides definiert der IEEE-802.3-Standard, auch bekannt als Ethernet-Standard. Zudem ist auch bekannt, dass diese Technologie mehr mit sich brachte als gedacht: MAC-Adressen sind fälschbar und Ethernet-Datenpakete können durch Switche abgefangen und manipuliert werden.

Aus der Sicht eines Kommunikationsteilnehmers bedeutet dies, dass seine Absicht, mit anderen Teilnehmern zu kommunizieren, in mehrfacher Hinsicht einer unerwarteten und nicht zu verhindernden Einflussnahme von außen unterliegt. Dazu gehören (0) das Auslesen von Inhalten eines Datenpakets, (1) das Abfangen und Manipulieren von Datenpaketen und (2) das Erfassen der Metadaten wie zum Beispiel Adressaten einer Kommunikation. Hier geht es also um Einflussmöglichkeiten im Bereich der Kommunikationsverarbeitung durch unberechtigte Dritte.

Auslesen & Manipulieren

GNUnet-Core verhindert die Ausformungen von Informationsmacht in Punkt (0) und (1) durch einen authentisierten Schlüsselaustausch und eine authentisierte Verschlüsselung, die Perferct Forward Secrecy (PFS) zur Verfügung stellt. Er baut nicht nur Links zwischen zwei Peers auf, sondern ist auch implizit für die

[73] Ich blende hier die etwas komplexe Verbindung zwischen GNUnet-Transport, GNUnet-ATS und GNUnet-Core aus.

Verbindungssicherheit (Authentizität, Vertraulichkeit, Integrität, Replay-Schutz) zuständig.

Dazu wird auf einem Host-Rechner mit einem installierten GNUnet-Peer eine kryptographisch generierte Adresse verwendet, welche die sogenannte Peer Identity (bestehend aus Public Private Key Pair) repräsentiert. Es handelt sich bei dieser Adresse um den Hash-Wert eines Public Keys, dessen Gegenstück der Private Key ist. Eine solche Adresse in Form einer HELLO-URI wäre zum Beispiel:

```
gnunet://hello/1G5Q5BAS7M708VFFH48JE0KHRWMDQ381Z1K9CB8NFZS3G7MN63R0
```

Kryptographische Adressierung

Zusammen bezeichnen sie also eine adressierbare kryptographische Identität, die für einen längeren Zeitraum gültig ist und auch als intrinsisch authentifizierbare Netzwerkadresse verwendet werden kann. Neben der Möglichkeit HELLO-URIs zu verwenden, können die Public Keys auch automatisch über HELLO-Nachrichten ausgetauscht werden.

Schlüsselaustausch und Verschlüsselung

Auf dieser Grundlage wird nun ein verschlüsselter Kanal mit PFS hergestellt. Dazu wird im Rahmen eines ECDHE-Schlüsselaustausches (a) ein kurzlebiges Schlüsselpaar erzeugt, (b) mit dem privaten Langzeit-Schlüssel der Identität signiert, (c) ein Schlüsselaustausch für die Berechnung des gemeinsamen Geheimnisses durchgeführt und (d) einige symmetrische Sitzungsschlüssel davon abgeleitet. Diese Sitzungsschlüssel werden nun für die symmetrische Kanalverschlüsselung als auch die authentisierte Integritätsprüfung verwendet. Zur Zeit beträgt die Lebendauer dieser Sitzungsschlüssel 12h, kann aber jederzeit durch die Initiative eines Peers erneuert werden.

Ein Sender kann so Inhaltsinformationen vor unberechtigten Akteuren geheim halten und die Manipulation von Daten verhindern. Hinzukommt, dass der Sender hinsichtlich Punkt (2) Kontrolle über seine Adresse hat: sie funktioniert sicher als Identität, Pseudonym oder temporäres Token, das verworfen werden kann und damit eine Form der Verkettungssicherheit ermöglicht.

Metadaten

Punkt (2) ist jedoch auch als Problem der Verkehrsanalyse – also die Analyse von Beziehungsstrukturen – bekannt und gilt als technische Herausforderung. Insofern dieses Problem jedoch nur von einer klugen Routing-Logik angemessen gelöst werden kann, ist es folglich weniger ein Problem vom GNUnet-Core-Dienst,

dessen Zweck ja die Verbindungssicherheit ist. Je nach Anwendung können hier unterschiedliche Methoden nach dem Stand der Wissenschaft zum Einsatz kommen. Im GNUnet-File-Sharing-Dienst wird Anonymität über das GNUnet Anonymity Protocol (GAP) erreicht. Ende-zu-Ende-Verbindungen nach dem Vorbild von TCP-Verbindungen, wie sie vom GNUnet-Dienst CADET bereitgestellt werden, sollen zukünftig Anonymität über Onion-Routing gewährleisten.

Gegen einen Man-in-the-Middle-Angriff, wie er im Ethernet mittels ARP-Spoofing möglich ist, schützt GNUnet-Core nur die Punkt-zu-Punkt-Kommunikation vor der Entschlüsselung. Eine simple Verkehrsanalyse aufgrund von Metadaten wäre daher ohne zusätzliche Maßnahmen möglich. Um diese Art der Angriffe abzuwehren, kommt GNUnet-Core der darunterliegende GNUnet-Transport-Dienst zur Hilfe, welcher eine Validierung der Peer-Adressen durchführt.[74]

Freiheitsgewinn

Damit wäre die technische Beschreibung für das Beispiel GNUnet-Core weitestgehend abgeschlossen und es lässt sich festhalten, dass GNUnet-Core im Rahmen seiner funktionalen Bestimmung jene sozial unerwünschten Folgen eines Ethernet-Protokolls aufhebt (und darüber hinaus anderen Risiken abfängt). *Der Nutzer wird dadurch in die Lage versetzt, selbstbestimmt zu kommunizieren, das heißt, über die Weitergabe von akteursbezogenen Informationen selbst zu bestimmen, ohne dass das technische Gerät seinen Interessen oder Erwartungen in dieser Hinsicht zuvorkommt und anderen Akteuren bedingungslos sensible Informationen zur Machtausübung zukommen lässt.*

Mit etwas Abstand betrachtet weist das Design der höheren Dienste wie beispielsweise GNUnet-R5N (zuständig für die Entfaltung eines Multihop-Netzwerkes) die gleiche Orientierung am Wert des Privaten auf: Hier wie dort werden Verschlüsselungs- und Anonymisierungstechniken in die feine Mechanik der Netzwerkprotokolle eingearbeitet, um die allgemeine Kommunikationsverarbeitung unter neue Bedingungen zu stellen und den Nutzerinnen und Nutzern einen höheren Grad an Freiheit bzw. Autonomie zu gewährleisten.

Machtverlust

Die hier auftretenden Machtverschiebungen als Folgeerscheinung sind klassisch und bereits gut erforscht. Am stärksten betroffen davon sind einzelne technisch

[74] Im Internet: https://gnunet.org/transport-ping-pong, Stand: 24.01.2016.

versierte Angreifer im Netzwerk, Netzwerk-Administratoren von Telekommunikationsanbietern bis hin zu Organisationen als Netzteilnehmer mit erheblichen rechtlichen oder ökonomischen Ressourcen – ihnen ereilt ein massiver Machtverlust. Für die Telekommunikationsanbieter wie AT&T, Saudi Telecom oder der Deutschen Telekom bedeutet dies konkret, dass ihre Organisationsmacht auf die banale Fähigkeit der Paketvermittlung reduziert wird.

Wir wollen uns nun der nächsten Klasse von Machtverschiebungen zuwenden. Lässt sich nämlich die Stärke der Logik des Privaten auf die besondere Umgangs*weise* mit akteursbezogenen Daten gründen, so sind ihr dort Grenzen gesetzt, wo es um die Verfügbarkeit oder Herrschaft über Algorithmen und Datenbanken geht.

2.2. Über den Machtverlust im Bezug auf Informationsverarbeitung

Die zweite Machtverschiebung ist bedingt durch die Logik des Antiautoritären und vollzieht sich im Bereich der IV. Genauer gesagt geht es um eben jene informationsverarbeitende Dienste, deren Funktionalität vollständig auf das Internet ausgerichtet ist und nebenbei das stille Sakrileg mit sich bringen, an Interessen und Entscheidungen von Organisationen gebunden zu sein. Der funktionale Zweck läuft dann Gefahr, im Gefecht der Interessen von Herstellern, Verwaltung, Systemherren, Klienten usw. unterlaufen zu werden. Mit der Logik des Antiautoritären ist nun gemeint, dass diese Informationsdienste radikal nach der Idee strikter P2P-Modelle gestaltet werden. Kein Peer ist dem anderen hinsichtlich seiner technischen Rolle überlegen, es herrscht Gleichberechtigung. Dabei kann jeder die gemeinsamen Ressourcen der anderen verwenden, vorausgesetzt, dass er auf lange Sicht etwas beisteuert. Die so entstehenden allmende-artigen *kooperativen Dienste* führen die IV dezentral und selbstorganisiert durch.

Beispiel: DNS vs. GNUnet-GNS

Ich möchte diesen Gedanken anhand einer beispielhaften Gegenüberstellung des Domain Name System (DNS) und dem GNU Name System (GNUnet-GNS) klarmachen. Das DNS dient im Grunde genommen der Übersetzung zwischen menschenlesbaren, einprägsamen Adressnamen und maschienenlesbaren Adressnummern. Es ist damit ein essentieller Dienst für viele Internet-Anwendungen,

die von Menschen genutzt werden. Technisch setzt es sich aus einer verteilten eindeutigen Datenbank und verschiedenen Protokollen zusammen, um diese Datenbank abzufragen oder sie zu synchronisieren. Trotz seiner verteilten Struktur besitzt es eine eingebaute Hierarchie von vertrauensbasierten Beziehungen, um Teile der Namensauflösung zu delegieren. Allein diese Entwurfsentscheidung, so zeigt Nathan Evans (2011, S. 4), kann bei bösartigen Verhalten oder wohlwollender Inkompetenz desaströse Auswirkungen haben.

Herrschaftssystem & Namensrechte

Der Betrieb von DNS beruht allerdings auch auf nicht-technischen Komponenten, nämlich (a) auf der Kontrolle des DNS-Namenraums und des IP-Adressraums durch die »Internet Assigned Numbers Authority« (IANA), die wiederum von der »Internet Corporation for Assigned Names and Numbers« (ICANN) verwaltet wird, (b) vertrauenswürdigen Registraren und (c) auf den Administratoren von autoritativen Namenservern und DNS-Resolvern. Die Verwaltung der Nutzungsrechte für global eindeutigen Namen werden von der obersten Institution ICANN an sogenannten vertrauenswürdige Registrierungsstellen delegiert. Für Namen unterhalb des Top-Level-Domain-Namen ».de« ist die deutsche Registrierungsstelle DENIC zuständig. Aber auch sie delegiert die Aufgaben der Registrierung an andere untergeordnete Registrare weiter.

Wer diese Rollen ausübt oder mittelbar kontrolliert, ist in der Lage, Einfluss auf die Verfügbarkeit und Zugänglichkeit von Namen (und den damit verbundenen Schlag an Informationen und Ressourcen) zu nehmen, andere Inhalte über falsche IP-Adressen auszuliefern oder das Nutzerverhalten anhand der DNS-Abfragen zu beobachten. Damit sollte klar sein, dass die IV im DNS summa summarum darin besteht, Namensrechte eines globalen Namensraums zu verwalten und Auskünfte zu geben. Und so folgt notwendig: wer die IV von Internet-Domain-Namen kontrolliert, kann Informationsmacht über andere ausüben.

In Großbritannien wurde diese Form der Informationsmacht, um nur ein Beispiel zu nennen, erst kürzlich im Fall einer zuvor frei zugänglichen Domain des Chaos Computer Clubs sichtbar, deren Inhalte als vorgeblich gefährlich oder unmoralisch bewertet wurden.[75] Ein anders Beispiel ist das Landgericht Köln, bei dem die Adresse

[75] Im Internet: https://www.ccc.de/de/updates/2014/ccc-censored-in-uk, Stand: 11.1.2015. An diesem Beispiel wird der Aspekt der

www.bag.de dem Bundesarbeitsgericht in einer Klage zugestanden und die ursprünglichen Besitzerin enteignet wurde.[76]

Verteilte kooperative Selbstverwaltung

Auf welche Art wird nun die IV vom GNUnet umgestaltet? Der GNUnet-Dienst GNS verzichtet gänzlich auf die oben beschriebenen autoritativen und hierarchischen Strukturen, indem es die Datenbank verteilt, selbstorganisiert und sicher auf Basis von DHTs und eines nutzerkontrollierten Identitätsmanagement-Systems betreibt. Anstatt eines global eindeutigen Namensraums mit einprägsamen Namen und dem System von autoritativen Stellen bietet GNS selbstverwaltete Namensräume an, auch lokale Zonen genannt, die jeder Nutzer mittels eines global einzigartigen Public Private Key Pairs kontrolliert. Technisch besteht eine Zone aus einem Satz assoziierter Namen und Adressen, die in Anlehung an das DNS in Form von Records abgelegt sind. Im GNS wird also für eine Namensabfrage sowohl der gesuchte Name selbst, als auch der Public Key der respektiven Zone benötigt.

Hinsichtlich der Umgestaltung der IV tritt nun ein weiterer entscheidender Punkt hinzu. Das GNS ermöglicht eine kooperative und soziale Praxis, bei der jeder Nutzer seine lokalen Zonen beziehungsweise Records auch mit anderen teilen kann, indem er den entsprechenden Public Key und die Records in der DHT veröffentlicht und sie somit adressierbar und anfragbar macht. Andere Nutzer können auf diese Weise für sie als vertrauenswürde eingestufte Zonen als Subnamensräume in ihre eigene lokale Zone integrieren. Erst dadurch wird es möglich, den eigenen willkürlich bestimmten Namensraum mit sozial bestimmten oder konventionellen Namensräumen zu kombinieren. So entsteht eine soziale Freiheit, »bei der die Freiheit des einzelnen [diejenige] ist, die die Freiheit des anderen erst ermöglicht.«[77] Diese erfährt allerdings ein zusätzliche Bestimmung, insofern der Nutzer mit der Integration eines fremden Subnamensraums die (eingeschränkte) Kontrolle über diesen Subnamensraum an jenen Urheber beziehungsweise Besitzer des Private Public Key Pairs überträgt. Zusammengenommen wird diese zentrale Eigenschaft im GNS auch

Informationsunterdrückung auch als Zensur bezeichnet.

[76] Im Internet: http://www.e-recht24.de/news/domainrecht/8207-domainrecht-gehoert-die-adresse-wwwbagde-dem-wwwbagde-dem-bundesarbeitsgericht.html, Stand 23.03.15.

[77] Honneth (2007, S. 37).

als »Delegation of Authority« bezeichnet. Im Gegensatz zum traditionellen DNS hat der Nutzer also die Macht, anderen Nutzern ein bedingtes Vertrauen zu schenken und ihre Namensräume mitzubenutzen oder aber das Vertrauen zu entziehen und einen anderen vertrauenswürdigen Namensraum einzusetzen.

Ein letzter Punkt sei im Zusammenhang mit der Informationsverarbeitung erwähnt. Mit der Idee der lokalen Namensräume und dem Konzept der »Delegation of Authority« wird auch dem expliziten Ziel der Zensurresistenz Rechnung getragen.[78] Das Zensieren von Worten und Gedanken wird allgemein in Form einer strukturellen Macht ausgeübt, wie zu Zeiten der Druckerpressen über die landesweiten Zeitungs- und Buchverlage. In dem Maße, wie es gelingt, den Dienst auf einzelne Peers zu verteilen, wird die Einflussnahme auf das Ganze, auf die Öffentlichkeit beziehungsweise Teilöffentlichkeiten und ihren Zugang zu Informationen auch schwieriger. Ein politisches System, das die Gesellschaft vermittels der Überwachung jedes einzelnen Individuums in die Zange nimmt, ist notwendig ein totalitäres.

Bis hier hin haben wir zwei emanzipatorische Konzepte kennengelernt: Einerseits verhilft die Möglichkeit, eigene Namensräume zu verwalten, zu mehr Selbstbestimmung und Freiheit, andererseits kann man Namensräume mit anderen teilen oder aber ihnen zuvor geschenkte das Vertrauen entziehen. Diese Eigenschaft ist auch als »Trust Agility« bekannt (und wird als ein großer Mangel der heutigen Public-Key-Infrastruktur[79] angesehen). Natürlich ist aufgrund des Gesagten offensichtlich eine neue soziale Praxis (und entsprechende nutzerfreundliche Tools) erforderlich und ich vermute, dass diese wohl erst durch die Hacker-Gemeinschaft in den kommenden Jahren geformt werden muss.

Durch diese Gegenüberstellung haben wir nun eine weitere Art kennen gelernt, wie das GNUnet-Projekt Informationsmacht thematisiert und auf sie einwirkt. Das realexistierende DNS und ihr System der Namensrechte werden aufgrund ihrer Vergangenheit und ihrer technisch-organisatorischen Verfasstheit als defizitäres bzw. illegitimes Herrschaftssystem bewertet. Die Informationsmacht des DNS wurde durch das aus zwei Komponenten bestehende soziotechnische System konstituiert:

[78] Vergleiche Wachs (2015, S. 184).
[79] Technisch bekannt unter dem Namen X.509 Certificate Authority Public Key Infrastructure.

einerseits einen von Menschen organisierten Verwaltungsapparat und die zugehörige Administrationsinfrastruktur, andererseits durch das Design der eingesetzten Technik. GNUnet-GNS hebt die Systemfolgen auf, indem es aus Sicht des Nutzers einen funktionsähnlichen, automatisierten und – in einer bestimmten Hinsicht – herrschaftsfreien Dienst »ins Leben gerufen hat«. *Die IV wird als dezentraler antiautoritärer P2P-Dienst neu instituiert.* War dies nur eine exemplarische Gegenüberstellung, so lässt sich diese Art der Machtverschiebung an weiteren Diensten des GNUnets durchexerzieren.

Im Prinzip kann man diese Folgenabschätzung auch für andere noch nicht »übersetzte« oder »umgestaltete« informationsverarbeitende Dienste treffen; die einzige Bedingung ist die *prinzipielle* Formalisierbarkeit von Entscheidungen und Verfahren, die einen Dienst zu einen Dienst machen. Ein Postdienst nimmt einen Briefumschlag entgegen, interpretiert die Adresse und stellt den Brief über bestimmte Postwege aus. Unter den Bedingungen der Turing-Galaxis[80] sind diese Dienstvorgänge in einer Weise formalisierbar und automatisierbar, dass funktionsähnliche Dienste ihn ersetzen können.

In politisch bedeutsamer Weise trifft diese Bedingung offenkundig auf Internetdienste zu, die in den Händen organisierter Informationsverarbeiter liegen wie Skype, Facebook, Youtube, Twitter, Yahoo, Dropbox oder Google.[81] Als Merkmal für »verdächtige« IV-Dienste kann gelten, dass sie eine zentral organisierte automatische Speicherung und Verarbeitung von Inhaltsdaten in der Hauptsache durchführen und extern bereitgestellte Kommunikationsinfrastrukturen als Basistechnologie verwenden (im Gegensatz zur KV, die *hauptsächlich* Kommunikationen als solche betrifft). Als weiteres Merkmal könnte geltend gemacht werden, dass vor allem *misbrauchstendenziöse* IV in den kritischen Blick des GNUnet-Projekts

[80] Ein früher Aufsatz zur Turing-Galaxis findet sich bei Coy (1994). Aktuell dazu auch Knaut et al. (2012).

[81] Aber auch ICANN, IANA und die Telkos in ihrer *Rolle* als organisierte Informationsverarbeiter für Adressen und Routen fallen unter diesen Topos. Man denke hier an das IP-Netz mit seinem IP-Adressen, das auf die Dienste der ICANN angewiesen ist, die sich wiederum auf die Kompetenzen der einzelnen Systemadministratoren von IP-Netzen (sog. Autonomer Systeme) verlassen müssen. Dass eine Einflussnahme auf diese Administratoren nicht unüblich ist, wird unter anderem auf `http://www.bgpmon.net` dokumentiert. Automatisierte antiautoritäre Adressvergabe- und Routing-Dienste werden bereits erforscht.

geraten. Das Computerspiel »World of Warcraft« in das GNUnet zu überführen wäre eine ehrwürdige Aufgabe, aber im Anbetracht der motivationalen Grundlage des GNUnet-Projekts wohl verhältnismäßig nachrangig.

2.3. Zwischenfazit

Theorie ähnelt in gewisser Weise einer entschlüsselnden Landkarte der Umgebung. Wir gewinnen eine Weitsicht über die möglichen Wege und damit verbundenen Vorteile und Schwierigkeiten je nach Beschaffenheit der Karte. Auch das breite Feld der Emanzipation von strukturellen Beschränkungen oder ideologieträchtiger Selbstzensur ist auf Theorie angewiesen zum Durchschauen von Abhängigkeit und Fremdbestimmung. Dazu gehört das von der Informatik verstärkte, komplexe Problem der Informationsmacht, denn das Internet und die daran angeschlossenen Rechenzentren und Endgeräte sind in ihrer jetzigen Form nicht nur schlecht durchschaubar, sondern auch ein Katalysator für Formen der Kontrolle, Überwachung und Zensur. An dieser Stelle setzt meine Analyse des GNUnet einschließlich ihrer sozialen Wirkung an. Die beiden hier typisiert beschriebenen Machtverschiebungen aufgrund technischer Veränderungen sind eine Hilfestellung für die zu erwartenden Folgen: So werden im Bereich der KV asymmetrische Machtverhältnisse zwischen legitimen Kommunikationspartnern und anderweitig beteiligten Akteuren einer Kommunikation abgebaut, während im Bereich der IV durch die Bereitstellung funktionsähnlicher Dienste diese Asymmetrien zwischen organisierten Informationsverarbeitern und den Nutzern ihrer Systeme abgebaut werden.

Die Technik zum Ausgangspunkt zu machen, ergab sich aus der Sache selbst, ansonsten hätten es bodenlose Spekulationen fern ihrer tatsächlichen Eigenschaften gegeben. Die Frage ist nur, wie wir einige Zweifel darüber loswerden können, das Problem der Informationsmacht ausreichend erfasst zu haben. Offensichtlich sind die Bereiche der IV und KV von besonderer Bedeutung und das allseits vernetzende Internet ein maßgeblicher Faktor. Was hier allerdings wenig Beachtung findet ist die Auseinandersetzung mit der gesellschaftlichen Bedeutung von Organisationen und ihren vielfältigen Formen der IV. Sie sind gleichsam wie die Technik ein Motor für gesellschaftliche Veränderungen. Indem wir die Hypothese vom Kopf auf die Füße

stellen und das Problem nicht von der Technik angehen, sondern hauptsächlich von den sozial(theoretisch)en Gegebenheiten, können wir den sozialen Veränderungsmöglichkeiten des GNUnet-Projekts Konturen verleihen. Ich meine, dass sich das Problem der Informationsmacht und sein Verhältnis zum GNUnet auf instruktive Weise durch eine zweite Landkarte eines unabhängigen Beobachters erschließen lässt und so möchte ich im letzten Teil die Theorie und Praxis des GNUnet-Projekts mit dem Datenschutzprojekt kontrastieren.

Teil IV.
Alternative Problemperspektive: Das Datenschutzprojekt

»Sind alle beherrschungsrelevanten Objekte und Bereiche zwecks Rationalisierung modellifiziert, so ist die ›informatisierte Gesellschaft‹ erreicht. Dies ist also nicht planmäßiges Werk kapitalistischer oder sozialistischer Bösewichte, wie viele in Unkenntnis der Mechanismen und der Komplexität hochindustrialisierter Gesellschaften vermeinen, sondern ist notwendiges Nebenprodukt der Verbindung von Informationstechnik, Telekommunikation und Rationalisierung von (Groß-)Organisation.« – Wilhelm Steinmüller

Im Folgenden möchte ich mich auf die Frage der Informationsverarbeitung konzentrieren. Dezentrierte Informationsverarbeitung gehört also zum paradigmatischen Kern des ausdrücklich an Werten orientierten GNUnet und sie soll der Folgenabschätzung entsprechend in jenen Bereichen eine umwälzende Wirkung entfalten, wo mächtige Akteure eine Herrschaft über Algorithmen und Datenbanken technisch, organisatorisch und ökonomisch aufrecht halten können. Die Dezentrierung organisierter IV ist mit anderen Worten nicht ein explorativer Selbstzweck, sondern ein zielgerichtetes ethisches Interesse. Aber welche Formen der organisierten IV sind davon inbegriffen und welche nicht? (Wie steht es mit Banken, Versicherungen, eGoverment-Diensten und ähnlichen Informationsverarbeitern, die sich mit dem Einzug des Internets ebenfalls wandeln?) Und woran macht sich fest, dass das Problem der Informationsmacht dann ausreichend behandelt wurde?

Um diese Fragen anzugehen werde ich zunächst im ersten Abschnitt einige Grundgedanken der Theorie des Datenschutzes vorstellen, die sich früh mit dem Verhältnis von gesellschaftlicher Macht und (digitaler) Informationsverarbeitung auseinandergesetzt hat und unter dem Vorzeichen des Internets heute weiterentwickelt wird. Hier betrachte ich dann auch die sozialen Strukturen näher, aus denen sich in weiteren theoretischen Erwägungen die gesellschaftlich notwendige Funktion von Organisationen und die Nützlichkeit ihrer Informationsverarbeitung ergibt. Das Zusammenwirken von Organisationen und Internet stellt unseren Blick für das Problem der Informationsmacht neu ein. Im zweiten Abschnitt werde ich versuchen, die Perspektiven des GNUnet- und des Datenschutzprojektes gegenüberzustellen und daraufhin wesentliche Gemeinsamkeiten und Differenzen festhalten. Auf dieser Grundlage mache ich einen Vorschlag, wie sich das GNUnet sinnvoll einordnen und beurteilen lässt.

1. Problemperspektive des Datenschutzprojektes

Was ist eigentlich das Problem des Datenschutzes und in welcher Weise wird es problematisiert? Dass es nicht (nur) um den Schutz von Daten geht, sondern in erster Linie um den Schutz »verdateter« Menschen – oder allgemeiner: Akteure –, ist

erst einmal eine banale Feststellung. Auf die frühe Phase des Datenschutzdiskurses der 1970er Jahre rückblickend, ging es dort um das unklare Verhältnis zwischen den Instanzen gesellschaftlicher Macht und Informationsverarbeitung.[82] Unter anderem vernahmen die damaligen Datenschützer Veränderungen im staatlichen (aber auch im wirtschaftlichen) Bereich, die ein neu entstehendes Machtgefälle innerhalb der Gesellschaft nach sich ziehen würden. Denn damals war zu befürchten, dass die Informatisierung bezüglich der staatlichen Institutionen eine Informationsmacht hervorbringen würde, die die rechtsstaatlichen Mechanismen der Gewaltenteilung weiter aushöhlen und in der Folge die Machtverschiebungen auf Kosten der Bürger bewirken könnte. Diese und ähnliche soziale Folgen einer rechnergestützten Informationsverarbeitung waren zu bedenken. Insofern aber die Entscheidung darüber, ob und wie die Technik für den gesellschaftlichen Gebrauch eingesetzt werden sollte, beim Menschen lag, handelte es sich bei diesem Problem in den Augen der Datenschützer um ein politisches: damals wie heute ging es darum, informationstechnischen Systeme *sozial beherrschbar* zu machen. Die Datenschützer erwogen damals, die sich anbahnenden informationstechnologischen Umwälzungen und ihre sozial unerwünschten Folgen gesamtgesellschaftlich über das Recht als soziales Steuerungsinstrument zu erfassen.

Martin Rost (2013b) erinnert in seinem Aufsatz »Zur Soziologie des Datenschutzes« an eben diese empirisch fundierten und gesellschaftstheoretisch angeleiteten Arbeiten. Daran anknüpfend formuliert er das Datenschutzproblem heute folgendermaßen: »Der gesellschaftstheoretisch zentrale Bezugspunkt für Datenschutzaktivitäten, der vor dem Datenschutzrecht liegt, weil das Recht bereits eine Reaktion auf den Machtkonflikt darstellt, ist [...] die *Konditionierung asymmetrischer Machtbeziehungen*, [...] *die spezifisch zwischen Organisationen und Personen im Kontext funktional differenzierter Gesellschaften vorliegen*« (S. 85). Er argumentiert dazu, dass die informationelle Selbstbestimmung in keiner ernsthaften Weise faktisch zu verwirklichen ist, wenn sie auf einer anthropologischen These wie dem Bedürfnis nach Privatheit gründet oder juristisch als Rechtsposition ermittelt wird, die sich an der dogmatischen Differenz öffentlich/privat aufhält; vielmehr ist zu ihrer tat-

[82] Steinmüller (1993, S. 190).

sächlichen Verwirklichung der Bezug auf bestehende Machtasymmetrien entlang von Konfliktlinien notwendig. Der Ansatz ist also, diese objektivistisch ermittelten Asymmetrien unter *Bedingungen* zu stellen, um auf Seiten der Schwächeren »Abwälzungen von Risiken«[83] abzufangen und Handlungsalternativen aufrecht zu halten – denn das ist es, was praktische Selbstbestimmung im Kern ausmacht. Wie aber lassen sich die (in informatisierten Kontexten situierten) Konfliktlinien und zugehörige Machtasymmetrien erfassen?

1.1. Organisationen

Nun, sie sind mit einem Worte strukturell gekennzeichnet. Dies bedarf einer kurzen Erläuterung bevor wir fortschreiten. Menschen können in flüchtige Beziehungen treten, wie die Praxis des Einkaufens und Bezahlens an der Kasse zeigt und dabei Ziele für das im engeren Sinne eigene Leben verwirklichen. Aber bereits in Gruppenbeziehungen kann das Zusammenwirken darin bestehen, ein größeres soziales Ziel zu erreichen. In einer Seminargruppe kann dieses soziale Ziel oder Bedürfnis darin bestehen, sich in einem hitzigen und anregenden Wissenschaftsdiskurs weiterzubilden. Davon abheben lassen sich Sozialstrukturen, deren soziale Funktion über die eigene Bedürfnisbefriedigung hinausgeht. Der Soziologe und Rechtswissenschaftler Manfred Rehbinder (2000, S. 37) differenziert dies folgendermaßen:

»Je nach Art der gegenseitigen Beziehungen in der Gruppe unterscheidet man zwischen Primärgruppen und Sekundärgruppen (Organisationen). Primärgruppen sind Kleingruppen (face-to-face-groups). Ihre sozialen Beziehungen sind eng, persönlich, intim. Unter Organisationen verstehen wir hingegen Gruppen, deren Mitgliedschaft durch ein rechtlich geregeltes Verfahren erworben werden und verlorengehen kann, die sich auf die Verfolgung

[83] Ein schönes Beispiel dafür findet sich bei Steinmüller (1993): Nehmen wir an, dass ein Betrieb mit vielen Angestellten in eine wirtschaftlich Schieflage gerät und sich dazu entschließt 10% der Angestellten zu entlassen, um Geld einzusparen. Der Betriebsleiter könnte seine Angestellten darüber informieren, dass in Kürze 10% der Leute zufällig ausgewählt und entlassen werden. Es wäre nicht unwahrscheinlich, dass sich daraufhin ein Generalstreik entwickelte. Nehmen wir zudem an, der Betrieb leistet einen Fahrtkostenzuschuss an alle. Der Betriebsleiter könnte alternativ die Daten seiner Angestellten nutzen, um die Fahrwege und Fahrtkosten zu ermitteln, die jeder Angestellte aufwenden muss. Mit einer statistischen Analyse ließe sich leicht eine Reduktion des Fahrtkostenzuschusses ermitteln, damit 10% der Leute nicht mehr das Geld haben, um zur Arbeit zu kommen. Das ist mit der »Abwälzungen von Risiken« gemeint.

spezialisierter Ziele und die Erbringung *bestimmter* Leistungen beschränken, hierarchisch und arbeitsteilig organisiert sind und Personen im Regelfall nur in zeitlich, sachlich und sozial *beschränkte* Hinsicht, nämlich in ihren Eigenschaften und Pflichten als Mitglieder dieser Organisation, in Anspruch nehmen. Organisationen sind zum Beispiel Wirtschaftsunternehmen, Verwaltungen, Kirchen, Krankenhäuser, Universitäten, Berufsverbände. Die sozialen Beziehungen in Organisationen sind im Vergleich zur Primärgruppe verhältnismäßig unpersönlich, mehr formell und auch seltener.«

Diese Beschreibung der inneren Beschaffenheit und Binnenstruktur müssen wir noch um einen weiteren Aspekt ergänzen. Nach außen ermöglicht die arbeitsteilige Gruppe/Organisation die Bearbeitung einer Vielzahl neuer Beziehungen zu Personen und Gruppen, die ihre spezialisierten Leistungen als »Klientel« in Anspruch nehmen, so dass Organisationen eben auch eine strukturelle Wirkung nach außen entfaltet. Wir wollen allerdings dem Verdacht einer bürokratischen Macht, die anonym im Hintergrund wirkt, nicht allzu viel Vorschub leisten und die Verschränkung von Struktur und Akteurshandeln dadurch erhellen, dass die hierarchische Ordnung innerhalb einer Organisation es sozialen Akteuren über strukturell bedingte Positionen ermöglicht, Entscheidungsmacht auszuüben. Wenn dies stimmt, lassen sich mindestens zwei Konfliktlinien bestimmen. Einerseits organisationsintern zwischen Unter- und Übergeordneten, andererseits zwischen Organisation und Klientel.

Diese Idee ist mehr oder weniger angelehnt an die These eines verschränkten Strukturalismus und Subjektivismus, wie sie auf gesellschaftstheoretischer Ebene unter anderem von Manuell Castells (2009, S. 14) vertreten wird:

»Societies are not communities, sharing values and interests. The are contradictory social structures enacted in conflicts and negotations among diverse and often opposing social actors. Conflicts never end; they simply pause through temporary agreements and unstable contracts that are transformed into institutions of domination by those social actors who achieve an advantagous position in the power struggle. [...] [The institutions, organizations and discourses] are crystallized power relationships; that is, the general means that enable actors to exercise power *over* other social actors in order to have the power *to* accomplish their goals. [...] Actors produce the institutions of society under the

conditions of the structural position that they hold but with the capacity (ultimately mental) to engage in self-generated, purposive, meaningful, social actions.«

Sind also Machtasymmetrien im Sozialen, die durch soziale Akteure wie Organisationen reproduziert werden, strukturell gekennzeichnet, drängt sich nun die Frage auf, was es mit den Organisationen im Kontext der Informatisierung der Gesellschaft genauer auf sich hat. Datenschutztheoretisch schlägt hier das Vorgehen durch, im ersten Schritt die gesellschaftlichen Strukturen, Akteure und Interessen zu untersuchen und anschließend jene Prozesse und ihre Folgen zu analysieren, die zunehmend informationstechnisch unterstützt werden (sollen).

Organisationen konzentrieren und organisieren Ressourcen in Form von Material, Personal und Motivationsmittel wie Geld, um eine Funktion/Aufgabe durch Arbeit zu erfüllen. Die Funktion, und damit ihr Zweck, ist nach sozialen Bedürfnissen ausgerichtet, die sich in einer arbeitsteiligen und politisch organisierten Gesellschaft ergeben. Organisationen sind daher ein wesentlicher Faktor der Reproduktionsbedingungen einer Gesellschaft.[84] Daraus folgt zum Beispiel, dass die Weitergabe persönlicher Informationen nicht immer eine allein selbstbestimmte Entscheidung ist, sondern Teil des kommunikativen Prozesses ist, um eine Dienstleistung in Anspruch zu nehmen, die vielleicht für den reibungslose Lebensvollzug eines Individuums nötig ist. Individuen können also bestimmten Organisationen nicht einfach nicht vertrauen, sie sind gesellschaftlich auf sie angewiesen. Allenfalls ist eine Wahl unter konkurrierenden Organisationen mit der gleichen sozialen Funktion möglich. Versicherung A kann gegenüber Versicherung B günstiger sein, weil sie das Geld bei den örtlichen Service-Kräften einspart und Call-Center einrichtet. Aber die zentrale Leistung beider Organisationen ist die selbe, nämlich das Individuum gegen bestimmte Lebensrisiken abzusichern.

Organisations-übermacht

Gleichzeitig wissen wir um die »gefährliche« Natur von Organisationen, den Einzelnen aufgrund seiner Abhängigkeit in Bedrängnis zu bringen, ohne dabei selbst an Eigenständigkeit zu verlieren. Ihre strukturelle Überlegenheit legt eine Risikoabwälzung nah, wo Internet-Großunternehmen durch den Verkauf von Kun-

[84] Das kann man sich auch daran klar machen, dass Institutionen als »Rückgrat des Sozialen« (Jaeggi, 2009a) unter anderem durch Organisationen verwirklicht werden. Vergleiche auch Rehbinder (2000, S. 47).

dendaten ihre finanzielle Notlage überbrücken können oder Behörden durch den gegenseitigen Austausch von personenbezogenen Informationen übermäßig neugierige und kritische Bürger einschüchtern.[85] Andererseits ergeben sich daraus auch Risiken für die Gesellschaft als Ganzes, wenn die strukturelle Übermacht für den Ausbau der Strukturen selbst genutzt wird oder bestehende gesellschaftliche Strukturen oder Institutionen, wie etwa der Demokratie, strukturell unterminiert werden. Gängige Praktiken sind Unternehmensübernahmen und Kooperationsverträge in der Wirtschaft oder gesetzlich legitimierter Informationsaustausch bei staatlichen Behörden.

1.2. … und ihre Informationsverarbeitung

Der Dienst der Informatik

Diese Situation verschärft sich dramatisch durch die Rolle der Informatik. Organisationen machen sich technisch gestützte Informationsverarbeitung zu Nutze, um Ressourcen, Prozesse und Klientel effizienter zu organisieren. Konkret bedeutet dies speziell für Personen, dass (a) Organisationen personenbezogene Informationen sammeln und Personenprofile als »Handler« erstellen, (b) Personenprofile optimieren durch Normierung zugrundeliegender Personenschemata, (c) statistische Daten sammeln, um weitere Personenschemata zu erstellen, die auf Personen übergestülpt werden können und (d) Personenprofile aufgrund ihrer Datenform weitergegeben werden können. Was hier spezifisch verwirklicht wird, ist allen voran eine effiziente Verwaltung von Personen. Im Bezug auf die Klientel ist eine persönliche Bekanntschaft nicht nötig (auch vorher schon nicht) und mit Hilfe von technischen Informationssystemen ist es möglich, die Menge der Beziehungen zu vergrößern und effizienter zu handhaben. (Diese Gesichtspunkte gelten auch für andere strukturell unterlegende soziale Akteure, wie im Falle einer von Staat überwachten Partei[86] oder NGO.) Mit den am Internet angeschlossenen Informations- und Kom-

[85] Das Fallbeispiel von Tim Gerber (2014) als Betroffener einer Datenschutzverletzung macht dies deutlich: »Wer sich für amtliche Informationen interessiert und Zugang zu den Behördendokumenten verlangt, erregt leicht das Interesse staatlicher Datensammler. Dabei lassen sich die Beamten kaum von bestehenden Datenschutzregeln bremsen, wie meine persönlichen Erfahrungen zeigen« (aus dem Abstrakt).

[86] Rath (2013).

munikationssystemen werden diese Möglichkeiten erneut potenziert, insofern die Verkettung von Informationen erleichtert wird.

An diesem Punkt zeigt sich sodann die doppelte Natur von organisierter Informationsverarbeitung: einerseits die Nützlichkeit von Verdatung und Datenverarbeitung, »ohne die eine moderne Gesellschaft im Grunde genommen nicht existieren könnte« (Steinmüller, 1993, S. 467), andererseits ihre verstärkende Wirkung auf die Organisationsübermacht, die ihren Ausdruck in einer aus den Fugen geratenen Informationsmacht erhält. Das hier zum Vorschein kommende politische Moment ist der Ausgangspunkt der Datenschutzaktivitäten. Was als gesellschaftlich nützliche IV angenommen wird,[87] soll unter politische Bedingungen gestellt werden, indem Organisationen gegenüber demokratisch legitimierten Datenschutzbeauftragten und gleichsam den Betroffenen nachweisen, dass sie die IV vollständig beherrschen, die personenbezogenen Daten »ausschließlich auf Fairness bedacht eng zweckbestimmt und vor allem sektorenspezifisch erheben und verarbeiten«.[88]

Versuchen wir nun den ursprünglichen Faden wieder aufzunehmen und die gewonnen Erkenntnisse über organisierte IV mit dem GNUnet in Beziehung zu bringen. Welche Schlussfolgerungen lassen sich ziehen? Sicherlich diese, dass wir die Folgenabschätzung zum GNUnet bezüglich der IV relativieren müssen. Organisationen sind nicht nur ein wesentlicher Teil der Reproduktionsbedingungen unserer Gesellschaft, sie erbringen auch Leistungen unterschiedlichster Art, die reine Internetdienstleistungen überschreiten und sich damit nicht auf funktionsähnliche herrschaftsfreie GNUnet-Dienste abbilden lassen. *Allein jene Organisationen, deren Funktion auf die Bereitstellung eines reinen Informations- oder Kommunikationsdienstes (allgemeiner: Internetdienst) spezialisiert sind, bewegen sich im Schatten dieses revolutionären Paradigmas.*

Mit der sozialanalytischen Datenschutzperspektive haben wir die blinden Flecke auf der Karte aufhellen können. Der Bereich der organisierten IV ist nicht allein durch die Logik des GNUnet-Projekts zu bewältigen – aber auch nicht allein durch die Bewältigungsstrategie des Datenschutzprojektes, wie wir nachfolgend sehen

[87] Für alle anderen gilt der Grundsatz, dass keine personenbezogenen Daten verarbeitet werden dürfen.

[88] Rost (2013b, S. 87).

werden.

2. Gegenüberstellung mit dem GNUnet-Projekt

2.1. Theorie und Praxis der Kritik von Informationsmacht

Stellt man nun die Problemperspektiven des Datenschutzes und des GNUnet-Projekts gegenüber, so behaupte ich, dass erstere tendentiell konstitutionskritisch und letztere tendenziell herrschaftskritisch arbeitet.[89] Für das GNUnet-Projekt bedeutet es, dass es eine Form der Kritik übt, die sich gegen die Fremdeinwirkungen einer hierarchisch übergeordneten und isolierten Macht auf den einzelnen Willen wendet. Die Konzeption von Macht ist hier die einer Herrschaft, die einschränkt anstatt zu ermöglichen.[90] Ob es die Telekommunikationsunternehmen sind, die VoIP-Dienste wie Skype blockieren, oder soziale Medien wie Facebook, welche die soziale Interaktion kontrollieren und anfallende Daten willkürlich weiterverwenden, oder die Exekutive und ihre Sicherheitsbehörden mit Zugriffsrechten auf Datensilos, um nur einige plakative Beispiele zu nennen. Kritik wird hier im Namen der Freiheit, unter Anrufung individueller Freiheitsrechte geübt. Bilden diese den normativen Maßstab der Kritik, so erhält sie ihre inhaltlichen Konturen in den theoretischen Angreifermodellen, in denen das Verhalten des Gegners analysiert und als falsch ausgewiesen wird, um letztlich konstruktiv-technisch behoben zu werden.

Im Kontrast dazu arbeitet der Datenschutz konstitutionskritisch, da er die Gesellschaftslogik und die darin enthaltenen sozialen Prozesse hinsichtlich der »konstitutiven Effekte« (Saar, 2009) analysiert, genauer gesagt, die spezifisch mit Informationstechnologien verbunden sind. Geknüpft an die demokratische Prämisse, nach welcher die politische Ordnung sich aus dem Zusammenspiel der Gestaltungswillen und -kräfte seiner Mitglieder bildet und legitimiert, steht hier ein Konzept von

[89] Dies wurde bereits von Seiten der Datenschützer wie Martin Rost und Wolfgang Zimmermann im Bezug auf das eigene Selbstverständnis erkannt, siehe Rost (2013a, S. 37).

[90] Eine solche Konzeption liegt beispielsweise der Rede von Seda Gürses zugrunde, wenn sie davon spricht, dass in PET-Diskursen die Organisation als Gegner verstanden wird. Vergleiche dazu Pohle und Knaut (2014, S. 227).

Macht als Konstitution im Vordergrund. In diesem Sinne schafft sie Freiräume, ermöglicht autonomes Leben, kanalisiert Kräfte. Insofern wird Gesellschaftlichkeit, verstanden als überindividuelle Lebensbedingung für individuelles und autonomes Leben, zu einer Machtfrage, bei der die positiven und negativen Folgen der Vergesellschaftung abzuwägen sind. Hinzu kommt, dass sich der Datenschutz historisch mit einer frühen Bindung an die Grundrechte und das Verfassungsrecht seine normativen Grundlage abgesichert hat, mit dessen Hilfe sozial unerwünschte Folgen kritisch untersucht werden konnten. Kritiktheoretisch wird hier aus der Analyse der funktional differenzierten Gesellschaft, also »einer breit angelegten Erzählung über die soziale Welt, die – soweit das möglich ist – überzeugend und wahr ist«,[91] und der Thematisierung von Risiken die Kritik entwickelt.

Damit aber enthält die Kritikform des Datenschutzes strukturalistische Argumente und Begründungen, die jedoch von den Betroffenen (als ihren Mandanten) aufgrund des notwendigen theoretischen Hintergrundwissens notorisch missverstanden oder unverstanden bleiben. Anders beim GNUnet-Projekt, das sich als PET individualistischer Argumentationen bedient, die auf eine individuelle, selbstbestimmte Nutzung von »Selbstschutz-Tools« hinausläuft. Von einer individualistischen Redeweise, wie es für diese Art der Kritik typisch ist, weicht sie sonderlicherweise ab, wo ihr Gegenstand – das GNUnet als Netzwerktechnologie – kategoriale Vorgaben macht: eine neue Vernetzungsform zu konstruieren ist ein grundlegend strukturalistisches Vorhaben, auch wenn dies nicht derartig theoretisiert wird. In diesem präzisen Sinne ergeben sich, ähnlich wie beim Datenschutzprojekt, konstitutive Effekte für gesellschaftliche Kommunikation, und damit für die sozialen Verhältnisse an sich.

Aber die unterschiedlichen Kritikformen haben noch eine andere theoretische Konsequenz, nämlich hinsichtlich des Problems von Organisationen. Das GNUnet-Projekt verordnet sich durch seine unversöhnlich widerstreitende, eben antagonistische Kritikform eine systematische »Blindheit« gegenüber der gesellschaftlichen Funktion von Organisationen.[92] Das vom Datenschutz herausgearbeitete spezi-

[91] Walzer (2009, S. 589).

[92] Dagegen regen die Diskussionsbeiträge der *Fundationes I* kritisch an, dass sich dieses Außerachtlassen der Organisation auch als eine »bewußte« strategische Aufgabenteilung begreifen lässt,

fische Problem der Organisationen ist offenkundig, wird aber so behandelt, dass entweder vollständig gegen sie gearbeitet wird im Sinne der Logik des Privaten und dem darin angewandten Angreifermodell *oder* ersetzend im Sinne der Logik des Antiautoritären mittels der Idee kooperativer Dienste. An dieser Stelle ist die konstitutionskritische Perspektive des Datenschutzes umfassender: Ausgehend von der Erkenntnis, dass gesellschaftlich relevante Kommunikation zwischen Organisationen und Personen stattfindet, muss sowohl die *Organisation* als auch das *Endnutzersystem* als auch die *Kommunikationsinfrastruktur* bestimmte Bedingungen erfüllen,[93] damit das tatsächliche Risiko der Informationsübermacht vermindert werden kann. Aus Sicht des Datenschutzprojektes ist das GNUnet also »nur« ein Teil der Lösung. Zwar gilt dies umgekehrt für das GNUnet-Projekt genauso, aber dort wird eben dieser Zusammenhang nicht thematisiert. Wie das Zusammenspiel der Aktivitäten in etwa aussehen kann, darauf werde ich im folgenden Abschnitt näher eingehen.

Als praktische Folge dieser unterschiedlichen Kritikformen lässt sich beobachten, dass auf der einen Seite die Datenschutzaktivitäten zur Umgestaltung der Gesellschaft ausgerichtet sind an der Rechtspolitik und der daran anschließenden Rechtsdurchsetzung und Technikgestaltung in ihrer institutionalisierten Rolle als behördliche und betriebliche Datenschutzbeauftragte, während andererseits die GNUnet-Mitglieder ihre gestalterischen Aktivitäten immer eng am softwaretechnischen Substrat durchführen, das seine eigene Verbreitungs- und Wirkungslogik hat.[94]

Ich möchte nun zur Beantwortung der zweiten und letzten Frage dieses Kapitels voranschreiten, ein Koordinatensystem für das Problem der Informationsmacht zu bestimmen, das für die Einordnung des GNUnet nützlich wäre und das Zusammen-

aufgrund derer sich die jeweiligen Aufgabenziele präziser umsetzen lassen. Man denke z. B. an individuelle Betroffenheit als Motiv, um Datenvermeidungstechniken im PET-Kontext radikal voranzutreiben.

[93] Vergleiche dazu die Beschreibung der drei Prozessdomänen bei Rost und Bock (2011, S. 33).

[94] Man denke z. B. an die Kopierbarkeit und Übertragbarkeit von Software (Verbreitungsaspekt) und die unmittelbare Wirkung von Verschlüsselungstechnik (Wirkungsaspekt) als Durchsetzung des Rechts auf Kommunikationsgeheimnis. Die Verbreitungslogik genauer zu beschreiben, ist eine eigene Untersuchung wert. Grundsätzlich ist die Richtung von der »Peripherie« (Internet-User) zum »Zentrum« (ISP-Switches, -Router).

spiel mit dem Datenschutzprojekt andeutet.

2.2. Technische Vorüberlegungen zum Zusammenspiel

Klar ist, dass das Internet das eng umrissene Problem der Informationsmacht von Organisation noch einmal massiv verschärft hat. Weil das Recht – und folglich auch das Datenschutzrecht – im Bezug auf die weltweit verteilte Kommunikation im Kontext organisierter Informationsverarbeitung seine Wirksamkeit zu verlieren begann, stiegen die Verkettungsrisiken für normierte Personendaten übermäßig an. Im Datenschutzdiskurs wurde dem dadurch Rechnung getragen, dass man Mitte der 2000er die PET-Entwicklungen bearbeitete und in die Datenschutzaktivitäten zu integrieren versuchte. So schreibt Rost (2008, S. 5) in seiner Arbeit über den Datenschutz im Anbetracht dieser Wechselwirkungen von Internet und Gesellschaft:

> »Progressive Datenschützer ließen sich deshalb zunehmend auf das Spiel mit dem Teufel oder zumindest mit dem Feuer ein: Sie suchten nach technischen Lösungen, um Datenschutz in Technik zu gießen und ihn, in technischer Infrastruktur geronnen, durchzusetzen«.

Das Spiel mit dem Feuer beziehungsweise mit den gefährlichen Internet-Technologien erinnert an die spekulative und verheißungsvolle Idee Alan M. Turings, als er Angesichts des Problems, die Enigma zu knacken, gesagt haben soll: »What if only a machine can beat a machine«. Uns regt es zu der Betrachtung an, das GNUnet als »Gegenfeuer« zu deuten und über das Zusammenspiel mit dem Datenschutz nachzudenken.

Für meine weiteren Überlegungen möchte ich mir ein analytisches Konzept zu Nutze machen, das Rost und Bock (2011, S. 33) für die technische Übersicht entwickelt haben. Sie schlagen vor, das rechnergestützte Informations- und Kommunikationssystem von Organisation und Klientel in drei Prozess-Domänen zu untergliedern: (a) ein Programm, das ausschließlich unter der Kontrolle des Nutzer ist, (b) ein Datenschutz-Management-System für Organisationen, das sowohl den Identitätsschutz des Nutzers und als auch die Interessen der Organisation berücksichtigt, und (c) eine gesellschaftliche IV- und KV-Infrastruktur, die neutral

gegenüber den Nutzern sein sollte, dabei Sicherheit und Anonymität technisch gewährleistet. Diese Dreiteilung ergibt sich aus dem Kriterium unterschiedlicher »Systemherren«, nämlich Nutzer, Organisation und technische Vermittler.

Wie kann nun das GNUnet hier hilfreich sein? Betrachten wir zu erst einmal (c). Wie ich bereits festgestellt habe, zielt das GNUnet-Projekt auf die Ersetzung des Internets als Infrastruktur ab (s. Abschnitt »Der Weg zum neuen Internet«). Das GNUnet ermöglicht sichere und dezentrale Ende-zu-Ende-Kommunikation und für einen Teil ihrer Dienste anonyme Kommunikation. Es ist bekannt, dass eine anonyme Kommunikationsinfrastruktur für Ende-zu-Ende-Kommunikation eine wichtige Voraussetzung für engere Kommunikationsbeziehungen ist. Zwar ist eine Anonymisierungstechnik wie GAP oder Onion-Routing bisher nicht in das Transportprotokoll GNUnet-CADET integriert worden, sie ist allerdings bereits in Planung.

Betrachtet man die Frage der Infrastruktur unter den derzeitigen Bedingungen etwas näher, gilt es zwischen den Nutzern und den Telekommunikationsversorgern zu unterscheiden. Das GNUnet-Projekt setzt auf das strikte P2P-Modell, so dass das GNUnet und seine Dienste auch an der »Peripherie«, also bei den Anschlusskunden, betrieben werden kann. Handelt es sich um ein drahtloses Maschennetzwerk (Wireless Mesh Network), kann die Infrastruktur vollständig vom GNUnet erzeugt werden. Dagegen verwenden Telekommunikationsversorger in ihren Netzen Backbone-Router und Switches, die üblicherweise mit einem Protokollstack bis OSI-Layer 3 operieren, und zwar mit MAC/ATM oder Ähnlichem auf Layer 2 und IPv4/IPv6 auf Layer 3 (ggf. BGP/RIP über TCP/UDP für das Routing zwischen Autonomen Systemen). Bis die GNUnet-Protokolle hier laufen, müssen sie wohl oder übel eine gewisse technische Reife erlangen. So gilt das bisher eingesetzte GNUnet-Routing-Protokoll R^{5}N-DHT gemäß den Autoren nur für Restricted-Route-Topologien, welche die Eigenschaften von Small-World-Netzwerke haben (mit einem Durchmesser von $O(log(n))$, wobei n die Anzahl der Knoten ist).[95] Die heutige Leistung des Internets hängt zudem mit den angeschlossenen Rechenzentren zusammen. Die P2P-Dienste des GNUnets wären mit diesen statischen Infrastruk-

[95] Vergleiche Evans (2011, S. 143).

turelementen wie beispielsweise dem Berliner Internet Exchange Point BCIX[96] kompatibel und würden dadurch noch zuverlässiger funktionieren (Beispiel: Replikation von Dateien im anonymen und dezentralen File-Sharing-Dienst). Abgesehen von der Installation und einem ordentlichen Upgrade-Management sind im Gegensatz zur Gemeinschaft der Tor-Relay- und Tor-Directory-Server-Betreiber keine weitere organisatorischen Aufgaben zu erfüllen.

Kommen wir nun zurück auf die drei Prozess-Domänen und betrachten (a) und (c), also die Nutzer und die Infrastruktur. Diese werden von den Autoren Bock und Rost nicht betrachtet, da ihr Fokus auf den Organisationen liegt. Hier entfaltet das GNUnet seine Wirkung gemäß den untersuchten Folgenabschätzungen aus Teil III mit den erkannten Einschränkungen im Bereich der organisierten IV (s. S. 80). Aber gerade hier kann es auf lange Sicht einige große Datenschutzkonflikte auflösen helfen, die mit Internetmonopolen aufgerissen wurden. Dabei gilt es zu betonen, dass dabei lediglich die technischen Bedingungen erschaffen werden – die soziale Migration bleibt an sich auf technische Migrationsmöglichkeiten (wie zum Beispiel facebook-Schnittstellen), attraktive Anwendungen, Aufklärungsarbeit und allgemeine Bewußtwerdung, bewegende Skandalereignisse und dergleichen angewiesen.

Schließlich gilt es noch einen letzten Fall (a–b–c) zu betrachten: Nimmt man nun hypothetisch an, dass eine Organisation mit einem legitimen sozialen Zweck über das GNUnet als Infrastruktur mit ihren Klienten kommuniziert, so können wir zwar mit Machtverschiebungen im Bereich der KV rechnen (s. S. 62), allerdings bliebe das Problem der Informationsmacht in Sinne des Datenschutzes bestehen. Es lässt sich schlicht ein Dienst nach dem Client-Server-Modell auf einem GNUnet-System betreiben, der als Kommunikationsendpunkt gegenüber dem Klienten dient. Hier fallen Daten im Zuge von personenbezogenen Verfahren an, die ausgerichtet an eben jenen legitimen Zweck als »gesellschaftlich relevanter Kommunikation« zu deuten sind (Prinzip der Zweckbindung). In diesen Fällen läuft es letztlich darauf hinaus, dass ein »Agent des Schwächeren« innerhalb der Organisation die Kommunikation unter Bedingungen stellen muss. Das heißt, um das Verkettungsrisiko

[96] BCIX: Berlin Commercial Internet Exchange, ein Rechen- und Datenzentrum mit höheren Routing-Kapazitäten.

durch die Verarbeitung und Speicherung von Informationen zu vermeiden als auch Datensparsamkeit und -Vermeidung zu betreiben, muss der Datenschützer im Allgemeinen auf nichtverkettbare Pseudonym- oder anonyme Credential-Techniken zurückgreifen, bei denen im Grenzfall (z. B. Haftungsfall) auch die Identität einer Person aufgedeckt werden kann.

Von Vertretern des Privacy-Paradigmas kommt an dieser Stelle meistens der Einwand, dass Privatheit mit der Möglichkeit der Identitätsaufdeckung verloren ist (s. S. 30). Intuitiv ist klar, dass eine Nachrichten-Webseite anonym lesbar sein sollte ohne rückwirkende Identitätsfeststellung. Ein Auto anonym über das Internet zu mieten verkennt jedoch das im Raum stehende Haftungsproblem, weshalb ein Autovermieter die anonyme Anfrage abweisen würde und die Gesellschaft auf diesen Dienst verzichten müsste. Aus diesem Grund muss die Abschätzung des Verfahrenszwecks und der Erforderlichkeit (a) von allen Beteiligten ausgehandelt werden, (b) transparent durchgeführt werden und (c) von zusätzlichen Instanzen wie Datenschutzbeauftragten oder Gerichten überprüft werden können.[97]

Die Datenschützer setzen hier als Lösung auf ein Datenschutz-Management-System auf Seiten der Organisation und auf ein nutzerkontrolliertes Identitäten-Management-System auf Seiten der Nutzer. Beide Systeme müssen von der Organisation bereitgestellt werden und nicht nur ihre eigenen Interessen, sondern gerade auch den Identitätsschutz des Nutzers berücksichtigen. Dies kann jedoch schwerlich aus der Perspektive des GNUnet-Projekts entwickelt werden, denn es erfordert die Auseinandersetzung mit der Organisation und ihrer gesellschaftlichen Funktion.

3. Vorschlag zur Einordnung und Bewertung des GNUnet

Mit den Anregungen von Martin Rost und Kristen Bock schlage ich die folgenden systematischen Konstellationen vor, für die sich der emanzipatorische Einfluss des GNUnet-Projekts abschätzen lässt. Siehe dazu Abbildung 2 auf der nächsten Seite.

[97] Rost (2012, S. 434).

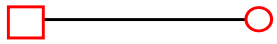
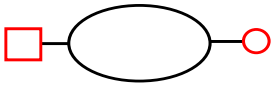
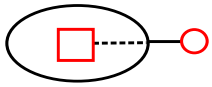
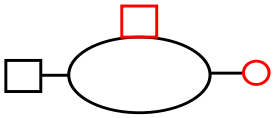
	Konstellation	Erklärung	Beispiele	GNUnet-Einfluss
α		Organisation führt vollständig die IV und KV durch	Bahnautomaten, Kameras im öffentlichen Raum	keinen
β		Organisation führt IV durch, nutzt Internet als Infrastruktur	eGovernment	IV: schwach KV: stark
γ		Organisation führt IV und partielle KV durch, reiner Internet-Dienst	facebook, google, Web-Mailer, dropbox, youtube	stark (da prinzipiell ersetzbar)
δ		Organisation führt KV durch, da Kontrolle über das Netz	Telekommunikationsanbieter	stark (da zensurresistent, dezentral, etc.)

Abbildung 2: Konstellationsdiagramm für das Problem der Informationsmacht. Kreis: strukturell unterlegener sozialer Akteur; Rechteck: strukturell überlegener sozialer Akteur bzw. Organisation; Ellipse: das Internet. Rot markiert sind die betrachteten Konfliktparteien.

Sie fasst fürs Erste das Ergebnis der letzten beiden Teile III und IV auf einem Blick zusammen.

Hier möchte ich meine anfängliche These veranschlagen, die ich zur Beantwortung der Machtfrage aufgestellt habe: Erst im Kontrast mit der Datenschutztheorie gewinnt das eigene Profil des GNUnet-Projektes Konturen, anhand derer sich nun bestimmte politische beziehungsweise gesellschaftliche Machtverschiebungen besser als zuvor in Teil III nachvollziehen lassen. Das Konstellationsdiagramm zeigt vier unterschiedliche Klassen von Beziehungen, die zwischen strukturell überlegenen (Rechteck) und strukturell unterlegenen (Kreis) Akteuren im Kontext vernetzter Gesellschaften auftreten können. Die rote Markierung zeigt dabei die relevanten Konfliktparteien. Die Modelle sind rekursiv auf die innere Struktur der Akteure (z. B. der Gruppe der Arbeitnehmer und Arbeitgeber *innerhalb* einer Organisation) anwendbar.

Im ersten Fall α führt eine der beiden Parteien die Informations- und Kommuni-

kationsverarbeitung innerhalb eines abgeschlossenen Systems vollständig durch und ist per Definition die strukturell überlegene Partei. Ein Beispiel hierfür wäre die Deutsche Bahn AG mit ihrem System von Servern, Datennetzen und Bahnautomaten. Eine Einflussnahme des GNUnets ist hier ausgeschlossen, sofern nicht Schnittstellen für persönliche Geräte geschaffen werden.

Im zweiten Fall β ist die Kommunikation zwischen zwei Akteuren bereits über das Internet vermittelt, so dass das GNUnet im Bereich der Kommunikationsverarbeitung einen starken Einfluss hat. Nun ist es aber so, dass es Organisationen gibt, die sich hinsichtlich ihrer Handlungs- und Arbeitsfunktionen nicht vollständig in funktionsähnliche GNUnet-Dienste übersetzen lassen und trotzdem eine gesellschaftsrelevante Funktion erfüllen. Eine solche Organisation wäre beispielsweise eine Behörde, die auf der Grundlage politischer und finanzieller Rahmenbedingungen Rechtsakte für Sozialleistungen durchführt. Hier kommt es aufgrund der Verwaltung der Bürger unvermeidlich zu einer datenschutzrelevanten Informationsverarbeitung.

Damit ist der dritte Fall γ bereits zum Anklang gekommen. Ist der Internetdienst einer Organisation im Prinzip vollständig berechenbar, also deren Handlungs- oder Arbeitsfunktionen in Algorithmen übersetzbar, ist er auch durch einen kooperativen verteilten GNUnet-Dienst austauschbar. Entsprechend treten hier zusätzliche starke Machtverschiebungen im Bereich der Informationsverarbeitung auf. Ein interessantes Beispiel könnte hier Amazon spielen. Die Idee eines virtuellen Marktplatzes, an dem Händler ihre Waren tauschen oder verkaufen, lässt sich auch als verteiltes System konzipieren. Die Entscheidung darüber, was angeboten oder verkauft werden soll, liegt bei den Händlern, Käufern und Tauschpartnern, also bei den Peers und nicht beim Dienst selbst!

Und schließlich bleibt der vierte Fall δ, der schlicht das Verhältnis sich Kommunikationsanbietern und seinen Nutzern widerspiegelt. In diesem leicht einzusehenden Fall wird die Rolle des Anbieters auf die Rolle eines agnostischen Paketvermittlers reduziert. Das GNUnet verhindern hier nicht nur die Entschlüsselung der Datenströme und die Analyse der Beziehungsstrukturen (soweit dies über die Anonymisierungsfunktionen implementiert oder angedacht ist), sondern vereitelt die Möglichkeiten der Zensur. Denn jegliche allgemeine Zensur von Inhalten müsste

darauf hinauslaufen, große Teile der Kommunikation schlicht zu unterbinden (s. File-Sharing).

Aus Sicht des Datenschutzes liegt in allen Fällen selbstverständlich ein Datenschutzkonflikt vor, der mit den Instrumenten, Methoden und Individualrechten des Datenschutzes gelöst werden muss.

Zusammenfassung

Das allgemeine Ziel der GNUnet-Entwicklung besteht darin, das Internet als Basistechnologie moderner Gesellschaften auf lange Sicht zu ersetzen. Diese Arbeit war der Versuch, das GNUnet als eine bestehende und sich weiterentwickelnde P2P-Netzwerktechnologie auf ihre emanzipatorischen Potentiale hin für Individuum und Gesellschaft zu untersuchen; oder, wenn man so will, ihren Einfluss auf die politische oder gesellschaftliche Ordnung zu verstehen und einzuschätzen lernen. Die entscheidende Einsicht dabei ist natürlich, bei massenhaft genutzten technischen Systemen von einem institutionellen Charakter auszugehen, der gesellschaftliche Handlungsmuster prägt. Um also dieses Vorhaben zu bewerkstelligen, bin ich zwei grundsätzliche Fragen nachgegangen: einerseits der Frage, welche ethische oder politische Motivationsgrundlage dem GNUnet-Projekt zugrunde liegt und wie der Sprung einer ethisch motivierten Problemsicht zur Technik vonstatten geht und andererseits die Frage, auf welche Weise die so entstehende Technik die soziale Realität zu verändern vermag. Zur Beantwortung der ersten Frage begann ich in Teil II damit, in einem ideologiekritischen und normativ-rekonstruktiven Verfahren die Selbstdarstellung des Projektes und seine normativen Wertvorstellungen herauszupräparieren, an denen sich die Technikgestaltung im Praxiszusammenhang orientieren sollte. Im Wesentlichen waren dies der *Wert des Privaten* und *des Antiautoritären* und jeweils davon abgeleitete logische Denk- oder Gestaltungsmodelle. Danach folgte die historische und systemtheoretische Darstellung des GNUnets, die sich mit dem zuvor Gesagten zu einem *technologischen Begriff* verbinden ließ. Die zweite Frage habe ich mit einer *Technikfolgenabschätzung* in Teil III beantwortet, die sich auf fruchtbare Weise sowohl an den herausgestellten Logiken des Privaten und des Antiautoritären entwickeln ließ, als auch an der analytischen Trennung zwischen *Informationsverarbeitung* und *Kommunikationsverarbeitung*. Beide Paare ließen sich insofern in Deckung bringen, als dass die Logik des Privaten traditionell auf vertrauliche und verkettungssichere Kommunikation abzielt, während die Logik des Antiautoritären das Augenmerk auf die Rückeroberung der (ehemals autoritativ organisierten) Informationsspeicherung und -verarbeitung legt, und zwar mit Hilfe lokaler und verteilten Ressourcen.

Ein zusätzlicher Schritt, der sich mir aufdrängte, war das Nachdenken über ein ähnlich ambitioniertes Projekt, dass sich meines Erachtens dem gleichen Problem illegitimer Informationsmacht verschrieben hatte. Mit dem Datenschutzprojekt und ihrer Verknüpfung aus Gesellschaftsanalyse und technischem Sachverstand habe ich in Teil IV ein umfassenderes Bild gezeichnet, anhand dessen ich den Folgenabschätzungen zum GNUnet schärfere Konturen geben konnte. *Vor allem dort, so die gewonnene Erkenntnis, wo Organisationen reine Internetdienste anbieten oder Organisationen als technische Vermittler Einfluss auf physische Netze haben, können starke Machtverschiebungen durch den Einsatz des GNUnets auftreten.* Schließlich zeigten die Überlegungen aus der Gegenüberstellung der beiden Projekte aber auch, dass beide zur Erreichung ihres Ziels, illegitime Informationsmachtverhältnisse unter neue Bedingungen zu stellen, einander benötigen.

Im Hinblick auf das anfangs gestellte Problem, wie denn der Weg des GNUnet-Projektes einzuordnen und zu bewerten sei, kann ich nur eine begrenzte Antwort geben: technisch lässt sich das GNUnet als eine Internet- beziehungsweise Basistechnologie für Informations- und Kommunikationsverarbeitung einordnen (s. S. 54). Die gesellschaftliche Einordnung und Bewertung seiner Auswirkungen hängt allgemein von den unterschiedlichen Werten und Interessen der betroffenen Gruppen oder Subjekte ab. Allerdings bieten die von mir hervorgehobenen normativen Maßstäbe des Datenschutz- und des GNUnet-Projektes in Abschnitt 2.1 eine gute Bewertungsgrundlage, insofern sie ethisch-politische (GNUnet) oder demokratische (Datenschutz) Begründungen liefern anstatt partikularistisch zu argumentieren. Hier gilt es jedoch weiter darüber nachzudenken.

Nicht zuletzt muss ich einem bedeutsamen Mangel im Bezug auf den Begriff der Informationsmacht Rechnung tragen. Denn mit Informationen über materielle und immaterielle Objekte lässt sich ebenfalls Macht auf Individuen und Gesellschaft ausüben. Diesen Umstand habe ich aufgrund der mir kompliziert erscheinenden Problemstruktur ausgeblendet. Ebenfalls nicht explizit behandelt habe ich den Aspekt der Zensur als Teilproblem informationeller Machtausübung, zumal einige vom GNUnet-Projekt entwickelte Techniken darauf eine Antwort zu finden suchen. Die freie Zugänglichkeit zu öffentlichen Informationen ist aber eine wichtige Transparenz- und Kontrollvoraussetzung für funktionierende Demokratien.

Epilog: Ansinnen für eine Politische Informatik

Wer die Diskurse über politische oder ökonomische Macht verfolgt, wird kritisch nachfragen: Was ist mit der Ausbeutung der Arbeit durch Kapital? Migrationsproblemen? Umweltproblemen? Wohnungskämpfen? Sexismus-, Homophobie-, und Xenophobie-Kämpfen? Faschismus-Kämpfen? Sind dies nicht viel wichtigere Schauplätze subjektiver und gesellschaftlicher Krisen? Das sind sie, und das Problem der Informationsmacht kommt eben hinzu. Machtstrukturen durchziehen auf vielfältige, überlappende und verschränkte Weise die Gesellschaft. Wie weit das Ausmaß von informationeller Macht auf Basis von Informationstechnologien gehen kann, deutet uns die folgende Passage von Manuel Castells (2004, S. 36) an:

> »Sicherlich gibt es große Gebiete auf der Welt und beträchtliche Bevölkerungsteile, die von dem neuen technologischen System ausgeschlossen sind: Das genau ist eine der zentralen Thesen diese Buches. Die Geschwindigkeit der technologischen Diffusion verhält sich selektiv, und zwar sowohl gesellschaftlich wie funktional. Der Zeitverzug beim Zugang zur Macht über die Technologie für Mensch, Länder und Regionen ist eine entscheidende Quelle der Ungleichheit in unserer Gesellschaft. Die ausgeschlossenen Gebiete sind kulturell und räumlich ohne Zusammenhang: Sie liegen in den US-amerikanischen Innenstädten oder in den französischen Banlieues ebenso wie in den Shanty Towns von Afrika oder in den unterentwickelten ländlichen Gebieten Chinas und Indiens. Doch die technologisch dominanten, gesellschaftlichen Gruppen und Territorien sind zu Beginn des 21. Jahrhunderts über den ganzen Globus miteinander verbunden [...].«

Daran ist mindestens zu erkennen, dass das Politische sich förmlich der Informatik aufdrängt. Mit der wachsenden Bedeutung der Informationstechnologien muss auch die Informatik neben dem bereits in einigen Teilen entwickelten ethischen Reflexionsstil, der auf den Umgang mit Menschen untereinander bedacht ist, oder einem moralischen, welcher der Technikentwicklung zum Kriegsgerät entsagt, notgedrungen auch eine politische Denkweise ausbilden. Die Kontrastierung mit der Datenschutzperspektive sollte unter anderem einen blinden Fleck im theoretischen Problemverständnis des GNUnet-Projektes thematisieren. Man kann diese Deutung zurückweisen und die Angreifermodelle als soziale Modelle für genügend erklären.

Aber dann bliebe es bei einer ethischen Haltung, welche die sozialen und politischen Zusammenhänge nicht diskutieren kann. Darin liegt auch der Grund, warum ich von einem zweideutigen ethisch-politischen Charakter des GNUnet gesprochen habe (s. S. 54). Dies ist kein Vorwurf, sondern vielmehr ein Nachweis für ein noch zu schaffendes Verständnis des Politischen innerhalb der Informatik. Nicht nur um die politischen Impulse zu verstärken und zu kräftigen, vielmehr jedoch um soziale und politische Theorien in den informatischen Reflexions- und Gestaltungsprozess einzubinden. Im Anbetracht der anstehenden Aufgaben, wie diese Arbeit exemplarisch zeigt, mangelt es in der Informatik an gesellschaftspolitischem Wissen. Die vorliegende Kritik hat somit – affirmativ gesprochen – mindestens die Berechtigung, ein Ferment für eine politische Informatik zu sein. Was kann das heißen? Dazu zwei Definitionen:

Informatische Politik, das sind jene menschlichen Handlungen, die durch den Einsatz von Informationstechnologien auf die politische und soziale Wirklichkeit Einfluss zu nehmen suchen. Bewertend füge ich hinzu, dass diese Handlungen weit verbreitet sind und ihr Einfluss meist unreflektiert bleibt. Die *Politische Informatik* hingegen bezeichnet jene Handlungen, die bei der Entwicklung und der Anwendung von Informationstechnologien nicht nur von ethisch-politischen Interessen oder Wertvorstellungen geleitet sind, um auf die politische und soziale Wirklichkeit Einfluss zu nehmen, sondern auch eine Theorie des Sozialen und des Politischen zugrundelegen.

Im Gegensatz zum GNUnet-Projekt verstehe ich das Datenschutzprojekt als ein genuin politisches, das die Gesellschaftsanalyse zum Ausgangspunkt nimmt und daraus die Bewältigungsstrategie der sozialen Beherrschbarkeit der Technik entwickelt und unter anderem das Recht als soziales Steuerungsinstrument dafür eingesetzt hat. Letzteres ist insofern nachvollziehbar, als dass die gesellschaftliche Funktion des Rechts die Bereinigung von Konflikten, Verhaltenssteuerung, Legitimierung und Organisation sozialer Herrschaft und die Gestaltung von Lebensbedingungen ist. Aber das Datenschutzrecht erbt damit auch all die Schwierigkeiten des Rechtssystems wie zum Beispiel die nachzüglerische Trägheit auf dem Trampelpfaden des technischen Fortschritts oder ihre manchmal komplexe und daher dysfunktionale Mechanik, die den Einzelnen vergrault. Jenseits dessen gibt es andere Beispiele für

proaktiven Datenschutz: rechtspolitisches Engagement, das »Unterfliegen« von Regeln (ohne das Recht bis zur Unkenntlichkeit zu beugen), Aufklärung und Beratung oder das Entwickeln eigener Projekte wie »AN.ON«.[98]

Die große politische Idee des GNUnet-Projekt, die es meines Erachtens zu würdigen und mit Elan zu verfolgen gilt, ist vielleicht keine so neue, aber für das radikaldemokratische Projekt ein wichtiger Baustein: das Ersinnen und Etablieren herrschaftsfreier kooperativer Internetdienste.

[98] Im Internet: https://www.datenschutzzentrum.de/material/themen/presse/anon.htm, Stand: 15.04.15.

Literatur

Altemeyer, Bob (2006): *The Authoritarians.* Winnipeg: Selbstverlag.

Anderson, Ross (1996): The eternity service. In: *Proceedings of PRAGOCRYPT*. Bd. 96, S. 242–252.

Banse, Gerhard; Armin Grunwald; Wolfgang König und Günther Ropohl (2006): *Erkennen und Gestalten. Eine Theorie der Technikwissenschaften.* Berlin: Resch-Buch, Scheßlitz.

Beneš, Nicolas (2014): *An Approach for Home Routers to Securely Erase Sensitive Data.* Diplomarbeit, Technische Universität München.

Bennett, Krista und Christian Grothoff (2003): GAP – practical anonymous networking. In: *Designing Privacy Enhancing Technologies*. Berlin, Heidelberg: Springer Verlag.

Bennett, Krista; Christian Grothoff; Tzvetan Horozov; Iona Patrascu und Tiberiu Stef (2002a): GNUnet – A truly anonymous infrastructure.

Bennett, Krista; Tiberius Stef; Christian Grothoff; Tzvetan Horozov und Ioana Patrascu (2002b): The GNet Whitepaper.

Bernstein, Daniel J. (2006): Curve25519: New Diffie-Hellman Speed Records. In: *Public Key Cryptography - PKC 2006*, Hg. Moti Yung; Yevgeniy Dodis; Aggelos Kiayias und Tal Malkin, Berlin, Heidelberg: Springer Verlag, Bd. 3958 von *Lecture Notes in Computer Science*, S. 207–228.

Bernstein, Daniel J.; Niels Duif; Tanja Lange; Peter Schwabe und Bo-Yin Yang (2012): High-speed high-security signatures. *Journal of Cryptographic Engineering*, Internet: http://dx.doi.org/10.1007/s13389-012-0027-1.

Castells, Manuel (2004): *Der Aufstieg der Netzwerkgesellschaft.* Opladen: Leske + Budrich.

Castells, Manuel (2009): *Communication Power.* New York: Oxford University Press.

Chaum, David (1981): Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90.

Coy, Wolfgang (1994): *Computer als Medien. Drei Aufsätze.* Techn. Ber., Universität Bremen.

Coy, Wolfgang (1996): Bauelemente der Turingschen Galaxis. In: *Informationsgesellschaft – Medien – Demokratie*, Hg. Edelgard Bulmahn; Kurt van Haren und Detlef Hensche. Marburg: Selbstverlag.

Coy, Wolfgang (2004): Was ist Informatik? Zur Entstehung des Faches an den deutschen Universitäten. In: *Geschichten der Informatik*, Berlin, Heidelberg: Springer Verlag, S. 473–498.

Crouch, Colin (2008): *Postdemokratie.* Frankfurt am Main: Suhrkamp.

Danezis, George und Claudia Díaz (2008): *A survey of anonymous communication channels.* Techn. Ber., Microsoft Research.

Danezis, George und Seda Gürses (2010): A critical review of 10 years of Privacy Technology.
Internet: http://vous-etes-ici.net/papers/DanezisGuersesSurveillancePets2010.pdf.
Der Tagungsband ist bis heute nicht veröffentlicht.

Demirović, Alex (2014): Eine Frage der Reife. Überlegungen zum Verhältnis von Ungehorsam und Demokratie. In: *Ungehorsam! Disobedience. Theorie & Praxis kollektiver Regelverstöße.* Leck: CPI Clausen & Bosse.

Diffie, Whitefield; Paul C. van Oorschot und Michael J. Wiener (1992): Authentication and Authenticated Key Exchange. *Designs, Codes and Cryptography*, 2:107–125.

Dingledine, Roger; Michael J. Freedman und David Molnar (2001): The Free Haven Project: Distributed Anonymous Storage Service. In: *Designing Privacy Enhancing Technologies*, Hg. Hannes Federrath, Berlin, Heidelberg: Springer Verlag, Bd. 2009 von *Lecture Notes in Computer Science*, S. 67–95.

Díaz, Claudia; George Danezis; Christian Grothoff; Andreas Pfitzmann und Paul Syverson (2004): Panel Discussion – Mix Cascades Versus Peer-to-Peer: Is One Concept Superior? In: *Privacy Enhancing Technologies*, Hg. David Martin und Andrei Serjantov, Berlin, Heidelberg: Springer Verlag, Bd. 3424 von *Lecture Notes in Computer Science*, S. 242–242.

Díaz, Claudia und Seda Gürses (2012): Understanding the landscape of privacy technologies. *Proceedings of the Information Security Summit*, S. 58–63.

Eudes, Yves und Christian Grothoff (2015): Créé pour tuer. *Le Monde*, 22009.

Evans, Nathan (2011): *Methods for Secure Decentralized Routing in Open Networks*. Dissertation, Technische Universität München, Garching bei München.

Evans, Nathan und Christian Grothoff (2011): Beyond Simulation: Large-Scale Distributed Emulation of P2P Protocols. In: *4th Workshop on Cyber Security Experimentation and Test (CSET 2011)*. USENIX Association, San Francisco, California.

Ferreira, Ronaldo A.; Christian Grothoff und Paul Ruth (2003): A Transport Layer Abstraction for Peer-to-Peer Networks. In: *Proceedings of the 3rd International Symposium on Cluster Computing and the Grid (GRID 2003)*. IEEE Computer Society, IEEE Computer Society,
Internet: http://grothoff.org/christian/transport.pdf.

GauthierDickey, Chris und Christian Grothoff (2008): Bootstrapping of Peer-to-Peer Networks. In: *Proceedings of DAS-P2P*.
Internet: http://grothoff.org/christian/bootstrap.pdf.

Gerber, Tim (2014): Erfahrungen mit dem Datenschutz in der Behördenpraxis. *c't Security*, S. 24–27.

Geuss, Raymond (2013): *Privatheit. Eine Genealogie*. Frankfurt am Main: Suhrkamp.

Greenwald, Glenn (2014): Hacking Online Polls and Other Ways British Spies Seek to Control the Internet.

Internet: https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet, Stand: 24.7.2014.

Grothoff, Christian (2003): Resource allocation in peer-to-peer networks. *Wirtschaftsinformatik*,
Internet: http://dx.doi.org/10.1007/BF03254946.

Grothoff, Christian (2011): The Free Secure Network Systems Group: Secure Peer-to-Peer Networking and Beyond. In: *SysSec 2011*. Amsterdam, Netherlands.

Grothoff, Christian (2013): The GNUnet Name System. Chaos Communication Congress 30C3.

Grothoff, Christian; Krista Bennett und Tzvetan Horozov. Lindgren (2003): An Encoding for Censorship-Resistant Sharing.

Grothoff, Christian; Ioana Patrascu; Krista Bennett; Tiberiu Stef und Tzvetan Horozov (2002): The GNet Whitepaper. *Purdue University*.

Grothoff, Christian; Bartlomiej Polot und Carlo von Loesch (February 2014): The Internet is Broken: Idealistic Ideas for Building a GNU Network. In: *W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)*. W3C/IAB, W3C/IAB, London, UK.

Honneth, Axel (2007): *Pathologien der Vernunft*. Frankfurt am Main: Suhrkamp.

Jaeggi, Rahel (2009a): Was ist eine (gute) Institution? In: *Sozialphilosophie und Kritik*, Frankfurt am Main: Suhrkamp.

Jaeggi, Rahel (2009b): Was ist Ideologiekritik? In: *Was ist Kritik?*, Frankfurt am Main: Suhrkamp.

Knaut, Andrea; Christian Kühne; Constanze Kurz; Jörg Pohle und Rainer Rehak, Hg. (2012): *Per Anhalter durch die Turing-Galaxis*. Münster: Monsenstein und Vannerdat.

Kurz, Constanze und Frank Rieger (2010): *Die Datenfresser*. Frankfurt am Main: Fischer Verlag.

Levy, Steven (2000): *Crypto: Secrecy and Privacy in the New Code War*. Bath: The Bath Press.

MacAskill, Ewen; Nick Davies; Nick Hopkins; Julian Borger und James Ball (2013): GCHQ intercepted foreign politicians' communications at G20 summits. Internet: http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits, Stand: 6.3.2015.

Morozov, Evgeny (2012): *The net delusion: The dark side of Internet freedom*. New York: PublicAffairs.

Müller, Andreas; Nathan Evans; Christian Grothoff und Samy Kamkar (2010): Autonomous NAT Traversal. In: *10th IEEE International Conference on Peer-to-Peer Computing (IEEE P2P'10)*. IEEE, Internet: http://grothoff.org/christian/pwnat.pdf.

Petersen, Harold Emanuel und Rein Turn (1967): System implications of information privacy. In: *Proceedings of the April 18-20, 1967, spring joint computer conference*. ACM, S. 291–300.

Pohle, Jörg (2014): Die immer noch aktuellen Grundfragen des Datenschutzes. In: *Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis*, Hansjürgen Garstka, Wolfgang Coy. Helmholtz-Zentrum für Kulturtechnik, Humboldt-Universität zu Berlin.

Pohle, Jörg und Andrea Knaut (2014): *Fundationes I: Geschichte und Theorie des Datenschutzes*. Münster: Monsenstein und Vannerdat.

Polot, Bartlomiej und Christian Grothoff (2014 2014): CADET: Confidential Ad-hoc Decentralized End-to-End Transport. In: *Med-Hoc-Net 2014*.

Rath, Christian (2013): Die Linke nicht länger am Pranger. Internet: https://taz.de/!109561/, Stand: 3.3.2015.

Rehak, Rainer (2011): *Angezapft: Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung.* Diplomarbeit, Humboldt-Universität zu Berlin.

Rehbinder, Manfred (2000): *Rechtssoziologie.* München: C. H. Beck.

Rehfus, Wulff D. (2003): *Handwörterbuch Philosophie.* Göttingen, Oakville: Vandenhoeck & Ruprecht / UTB.

Rivest, R. L. und B. Lampson (1996): SDSI – a simple distributed security infrastructure.

Rolf, Arno (1992): Sichtwechsel – Informatik als (gezähmte) Gestaltungswissenschaft. In: *Sichtweisen der Informatik. Theorie der Informatik*, Hg. Wolfgang Coy, Braunschweig; Wiesbaden: Vieweg.

Rost, Martin (2008): Gegen große Feuer helfen große Gegenfeuer, Datenschutz als Wächter funktionaler Differenzierung. *Vorgänge*, 184:15–25.

Rost, Martin (2012): Standardisierte Datenschutzmodellierung. *Datenschutz und Datensicherheit*, 6:433–438.

Rost, Martin (2013a): Neun Thesen zum Datenschutz. In: *Fundationes I: Geschichte und Theorie des Datenschutzes*, Hg. Jörg Pohle und Andrea Knaut. Münster: Monsenstein und Vannerdat.

Rost, Martin (2013b): Zur Soziologie des Datenschutzes. *Datenschutz und Datensicherheit*, 2:85–91.

Rost, Martin und Kirsten Bock (2011): Privacy By Design und die neuen Schutzziele. *Datenschutz und Datensicherheit*, S. 30–35.

Saar, Martin (2009): Macht und Kritik. In: *Sozialphilosophie und Kritik*, Hg. Rainer Forst; Martin Hartmann; Rahel Jaeggi und Martin Saar. S. 567–587.

Scahill, Jeremy und Glenn Greenwald (2014): The NSA's Secret Role in the U.S. Assassination Program.

Internet: https://firstlook.org/theintercept/2014/02/10/the-nsas-secret-role/, Stand: 6.3.2015.

Scott, James C. (1999): *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.* New Haven, London: Yale University Press.

Silberschatz, Abraham; Peter Baer Galvin und Greg Gagne (2010): *Operating System Concepts.* John Wiley & Sons Pte Ltd.

Steinmüller, Wilhelm (1993): *Informationstechnologie und Gesellschaft. Einführung in die angewandte Informatik.* Darmstadt: Wissenschaftliche Buchgesellschaft.

Totakura, Sree Harsha (2013): *Large Scale Distributed Evaluation of Peer-to-Peer Protocols.* Diplomarbeit, Technische Universität München.

Toth, Gabor X (2013): *Design of a Social Messaging System Using Stateful Multicast.* Diplomarbeit, University of Amsterdam, Faculty of Science, System and Network Engineering.

ULD, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2009): Interviews zur Geschichte und Programmatik des Datenschutzes in Deutschland: Wilhelm Steinmüller. Geführt von Martin Rost.

Vidal, John und Suzanne Goldenberg (2014): Snowden revelations of NSA spying on Copenhagen climate talks spark anger.
Internet: http://www.theguardian.com/environment/2014/jan/30/snowden-nsa-spying-copenhagen-climate-talks/, Stand: 6.3.2015.

Wachs, Matthias (2015): *A Secure and Resilient Communication Infrastructure for Decentralized Networking Applications.* Dissertation, Technische Universität München, München.

Wachs, Matthias; Martin Schanzenbach und Christian Grothoff (2014): A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System. In: *International Conference on Cryptology and Network Security (CANS).* Berlin, Heidelberg: Springer Verlag.

Walzer, Michael (2009): Gesellschaftskritik und Gesellschaftstheorie. In: *Sozialphilosophie und Kritik*, Frankfurt am Main: Suhrkamp.

Winograd, Terry und Fernando Flores (1989): *Erkenntnis – Maschinen – Verstehen.* Berlin: Rotbuch-Verlag.