Teil II
Kryptographie & Gesellschaft

Die ersten zwei Kapitel haben sich mit der Kryptographie aus technologischer Perspektive beschäftigt. Kapitel 1 hat die geschichtlichen Ursprünge der Kryptographie beschrieben, wobei die Bedeutung verschlüsselter Kommunikation für Militär, Diplomatie und Geheimdienste hervorzuheben war. Kapitel 2 hat anschließend den Paradigmenwechsel hin zu einer Modernen Kryptographie erläutert – einer Kryptographie, die rigoros mathematisch gedacht und heute ubiquitär genutzt wird. Diese technologische Realität der Modernen Kryptographie ist Voraussetzung und Rahmenbedingung für Teil II. Basierend darauf wird die grundlegende These vertreten, dass Kryptographie auch eine *sozial-gesellschaftliche Angelegenheit* ist. Sie ist über die technologischen Aspekte hinaus eingebettet in soziale und gesellschaftliche Strukturen, Ideen und Vorstellungen. So wie für eine Ethik von Artificial Intelligence (AI), Bioethik, Medizinethik oder Umweltethik gilt, dass sie in ihrer Anwendung immer einen Bezug auf Technologie und Gesellschaft erfordert, so ist das, wie sich im Folgenden zeigen wird, auch für eine Ethik der Kryptographie der Fall. Damit wird Teil II zwar methodisch deskriptiv bleiben, allerdings wird sich diese Deskription nun an vielen Stellen auch auf normative Argumente und Aussagen beziehen.

Der hier vorgestellten Ethik der Kryptographie liegt zudem keine rein deduktive Argumentation zugrunde, die von einer einzelnen ethischen Theorie lediglich abzuleiten versucht, was für den Umgang mit Kryptographie zu gelten hätte. Denn eine rein deduktive Argumentation läuft in dem Fall Gefahr, sich von den Möglichkeiten der Wirklichkeit zu entfernen. Wenn bereits bestehende und gesellschaftliche Normen angenommen und in einen Anwendungsfall gezwungen werden, kann die eigentliche *Intention* und *Begründung* eben jener Norm verloren gehen. Um nur ein Beispiel zu nennen: Wenn das Briefgeheimnis für private Kommunikation gilt, wie verhält sich diese Norm im *digitalen* Rahmen? Kann eine solche Norm direkt angewandt werden, oder erzeugt nicht die Realität des Digitalen eine Situation, in der selbst die Norm – im dialektischen Sinne – neu beurteilt werden sollte? Spätere Kapitel werden analysieren, dass dies durch den beschriebenen Paradigmenwechsel

insbesondere für eine Ethik der Kryptographie von Relevanz ist.[1] Eine Perspektive auf die gesellschaftlichen Zusammenhänge der Kryptographie wird der Argumentation helfen, normative Problem- und Fragestellungen zu identifizieren, um sie anschließend lösen und beantworten zu können.

Dieser Methodik folgend wird sich Teil II mit zwei Themen an der Schnittstelle von Kryptographie und Gesellschaft auseinandersetzen. Zunächst untersucht Kapitel 3 den Cryptoaktivismus als eine neue Form des Aktivismus, der erst möglich wurde durch den technologischen Paradigmenwechsel hin zur Modernen Kryptographie. In diesen Aktivismus wird mit der Software *Pretty Good Privacy* (PGP) beispielhaft eingeführt. Anschließend soll der Cryptoaktivismus anhand von Motiven, Zielen und Mitteln systematisiert werden. Zuletzt stellt dieses Kapitel die bekannteste Strömung an der Schnittstelle von Gesellschaft und Kryptographie vor: die Cypherpunks. Diese hatten stets eine eigene, normative Vorstellung über die Kryptographie, deren normative Begründungen in Teil III der Arbeit vertiefter zu diskutieren sein werden. Ein Teil dieser Vorstellung war oftmals, dass Kryptographie kaum oder nicht regulierbar sei.

Hieran anknüpfend wird Kapitel 4 systematisch analysieren können, dass Kryptographie für die meisten Menschen doch auf verschiedene Art und Weise erfolgreich regulierbar ist. Dazu wird methodisch eine analogische Parallele der Regulierung des Internets und der Regulierung der Kryptographie hilfreich sein. Zu dieser regulatorischen Systematik sind vor allem die theoretischen Arbeiten von Lawrence Lessig (*Code: Version 2.0*) sowie Jack Goldsmith und Tim Wu (*Who Controls the Internet?*) zu diskutieren.[2] In diesem Kontext können anschließend die sogenannten *Crypto Wars* eingeordnet werden, womit bereits normative Problemstellungen aus Teil III angedeutet werden sollen.

Zusammenfassend wird Teil II argumentieren, dass der *gesellschaftliche* Umgang mit Kryptographie immer auch eine *Entscheidung* voraussetzt. Ob Individuen vertraulich kommunizieren können, ob sie Verschlüsselung im Alltag verwenden, ob sie auf nutzbare Kryptographie zugreifen können – all das ist immer auch an eine Entscheidung geknüpft, wie Politik und Gesellschaft mit Kryptographie umgehen möchten. Zwar

1 Siehe insbesondere Kapitel 5. Vor allem ist dabei nach Theorien angewandter Ethik zu fragen, die sich in ein *Top-down*- und ein *Bottom-up*-Modell einordnen lassen.

2 Siehe Lessig, *Code*; in der ersten Version auch Lawrence Lessig. *Code: And Other Laws Of Cyberspace*. New York: Basic Books, 1999. Siehe außerdem Goldsmith und Wu, *Who Controls the Internet?*.

sind in diesem Teil noch keine abschließenden normativen Analysen der unterschiedlichen Möglichkeiten von Entscheidungen vorzunehmen. Unterschwellig werden aber viele der normativen Optionen klarer werden, wenn wir das Verhältnis von Kryptographie und Gesellschaft diskutiert und definiert haben.

3 Aktivismus und Kryptographie

> Maybe there will be anarchy, maybe even chaos. But chaos at least has an open architecture. Chaos has always been the native home of the infinitely possible.
>
> – John Perry Barlow, Mitgründer der *EFF*[1]

Phil Zimmermann, geboren 1954 und aufgewachsen in Florida, bekleidete keine höheren politischen Ämter, gründete keines der heute erfolgreichen Big-Tech-Unternehmen, genoss auch keine Ausbildung an einer Eliteschule.[2] Sein Leben unterscheidet sich in den biographischen Daten von dem jener Kryptographen, die wir in den vorherigen Kapiteln kennengelernt haben. Diffie und Hellman waren respektierte Persönlichkeiten an der angesehenen Stanford University, Rivest, Shamir und Adleman wirkten am nicht weniger reputablen Massachusetts Institute of Technology. Auch mit den Kryptographinnen und Kryptographen der Geheimdienstorganisationen und militärischen Institutionen, die die Forschung jahrzehntelang geprägt hatten, hatte Zimmermann wohl wenig gemein.

Aber gerade deswegen wurde Zimmermann zum Archetyp des *Cryptoaktivismus*. Sein Handeln als Einzelperson konnte ganze Nationen, Unternehmen und schließlich die Gesellschaft beeinflussen, womit er vielleicht sogar eine Art *Crypto-Singularität* einzuleiten vermochte.[3] Dieses sehr spezifische Verhältnis von Aktivismus und Kryptographie ist dabei eine neuartige Erscheinung, die erst durch den Paradigmenwechsel hin zur Modernen Kryptographie möglich wurde. Auch deswegen ist solcher Aktivismus in der akademischen und ethischen Forschung bislang wenig beachtet worden.

Dieses dritte Kapitel soll daher nach einer Diskussion um Phil Zimmermanns Wirken (Abschnitt 3.1) systematisch eruieren, welche Motive,

1 Siehe John Perry Barlow. *A Pretty Bad Problem: Forward to PGP User's Guide by Phil Zimmerman*. 1995. URL: https://www.eff.org/de/pages/pretty-bad-problem (besucht am 15.04.2024). Die *EFF* ist die *Electronic Frontier Foundation*.

2 Zu seinen biographischen Daten siehe Levy, *Crypto*, S. 187–191, sowie Maureen Webb. *Coding Democracy: How Hackers Are Disrupting Power, Surveillance, and Authoritarianism*. Cambridge, MA, und London: MIT Press, 2020, S. 44–46.

3 Diese Einschätzung der Crypto-Singularität geht zurück auf Tim May, zitiert in Jarvis, *Crypto Wars*, S. 39, vgl. S. 221, zur Diskussion auch S. 39–41.

Ziele und Mittel dem Cryptoaktivismus gemein sind und was einen solchen Aktivismus generell charakterisiert (Abschnitt 3.2). Im Anschluss wird mit den *Cypherpunks* und einer sogenannten *Crypto-Anarchie* eine spezielle und radikale Form dieses Cryptoaktivismus vorgestellt (Abschnitt 3.3).[4]

3.1 Pretty Good Privacy (PGP)

In allen Facetten des Cryptoaktivismus bleibt Phil Zimmermann das Paradebeispiel für das Verhältnis von Kryptographie, Gesellschaft und Politik. Die Bedeutung von Zimmermanns Wirken liegt nämlich nicht mehr in einer *theoretischen* Grundlegung eines neuen Paradigmas der Kryptographie, sondern vielmehr in einer *praktischen* Realisierung einer solchen Kryptographie.[5] Das, was Diffie und Hellman sowie Rivest, Shamir und Adleman theoretisch begonnen hatten, erreichte durch Phil Zimmermann die Endgeräte von Millionen von Menschen. Was war aber nun seine Idee, die ihm gar den schmeichelhaften Titel als „America's first crypto-criminal"[6] einbrachte? Die Antwort darauf sind drei Buchstaben: *PGP*.

PGP steht für *Pretty Good Privacy*[7] und ist eine Software zur Verschlüsselung von E-Mails, welche die kryptographische Theorie von Diffie und Hellman sowie von Rivest, Shamir und Adleman auch praktisch implementiert und nutzbar macht.[8] Zimmermann finalisierte eine erste Version der Software im Jahr 1991.[9] Wenige Zeit später bildete sich eine

4 Auch Levy spricht im Kontext der Cypherpunks von Cryptoaktivismus; siehe Levy, *Crypto*, S. 205. Diese Arbeit wird den Begriff jedoch umfassender definieren.

5 Nicht zu verkennen ist hierbei die Parallele zu Kuhns zweitem Kriterium, durch das ihm zufolge eine Leistung zum Paradigma wird. Diese Leistung sei „sufficiently open-ended to leave all sorts of problems for the redefined group of practitioners to resolve". Just in dieser Charakteristik ist (unter anderem) Zimmermanns Wirken eingebettet, insofern er als Praktiker einige Folgeprobleme des Paradigmas lösen konnte. Kuhn, *The Structure of Scientific Revolutions*, S. 11.

6 Andy Greenberg. *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers*. New York: Plume, 2012, S. 76.

7 Eine Bezeichnung in Anlehnung an einen fiktionalen Sponsor von Garrison Keillors Radiosendung *A Prairie Home Companion*. Siehe Levy, *Crypto*, S. 194–195.

8 Siehe einführend zu PGP Bauer, *Secret History*, S. 509–518.

9 Siehe Jarvis, *Crypto Wars*, S. 218.

Community zur Weiterentwicklung von PGP.[10] Zwar war Zimmermann nicht der Einzige, der an einer solchen Software gearbeitet hatte.[11] Das Besondere an seiner Arbeit war jedoch, dass PGP später frei zugänglich wurde[12] – für *jeden*. Denn PGP verfolgt einerseits die Philosophie, dass die bestmöglichen Verfahren zur Kryptographie bereitgestellt werden sollen; andererseits schreibt PGP den Nutzenden möglichst wenig vor.[13] PGP wurde somit das damals mit Abstand bekannteste Programm zur verschlüsselten Kommunikation.[14]

Wie der Journalist Steven Levy schreibt, war seine Motivation getrieben durch „scientific curiosity, a hobbyist's passion, and a bit of political paranoia"[15]. Obgleich er ursprünglich auch monetäre Hoffnungen gehabt hatte – er hatte über die Möglichkeit von *shareware* nachgedacht –, sah er später aus politischen Gründen davon ab und entwickelte PGP als *freeware*.[16] Doch mit dieser Freiheit und einem schnellen Erfolg von PGP hatte Zimmermann nicht nur Unterstützerinnen und Unterstützer gewinnen können. Gerade *wegen* dieses Ansatzes einer frei verfügbaren Software folgten auf PGP teils heftige Rechtsstreitigkeiten und mediale Diskussionen.[17]

Einerseits war da die Auseinandersetzung mit denjenigen, die zwar auch an Verschlüsselungssoftware gearbeitet hatten, diese allerdings lizenzieren wollten. Ein frei zugängliches PGP war für eine kommerziell ausgerichtete Firma natürlich ein ökonomisches Problem. Warum sollte jemand eine kostenpflichtige Software erwerben wollen, wenn die gleichen Algorithmen in einer freien Software bereits implementiert waren?[18] Dies hatte schließlich einen Rechtsstreit um Lizenzierung und Patente zur

10 Siehe Levy, *Crypto*, S. 200.

11 Insbesondere ist hier *RSA Data Security* und deren Programm *Mailsafe* zu nennen; siehe ebd., S. 193.

12 Siehe ebd., S. 196–198.

13 Siehe Beutelspacher, *Geheimsprachen und Kryptographie*, S. 73.

14 Siehe ebd., S. 73.

15 Levy, *Crypto*, S. 187.

16 Siehe ebd., S. 195–196.

17 Zur Einführung in diese medialen Diskussionen siehe Jarvis, *Crypto Wars*, S. 224–228; zu medialen Rezeptionen im Kontext der frühen Crypto-Anarchie auch Rid, *Rise of the Machines*, S. 263–265.

18 Dass die Sachlage komplexer ist, als diese rhetorische Frage vermuten lässt, zeigt die heutige Situation, in der Open Source und kommerzielle Anwendung nicht mehr im Widerspruch zueinander stehen. In der Realität spielen zahlreiche Faktoren eine Rolle, so etwa Nutzbarkeit, Lobbyismus, Supportmöglichkeiten, Haftbarkeit usw.

Folge, insbesondere mit Jim Bidzos vom Unternehmen *RSA Data Security*, das auf die Entwickler des gleichnamigen Algorithmus zurückging.[19]

Zum anderen gab es einen Disput mit der US-amerikanischen Regierung. Diese und insbesondere die NSA hatten vor dem Paradigmenwechsel der Kryptographie eine Vormachtstellung im Bereich kryptographischer Forschung und Nutzung inne.[20] Eine Software wie die von Zimmermann, die „Encryption for the Masses"[21] bot, war auch für die NSA ein Novum in der Geschichte. Für Zimmermann jedoch sollte PGP eine „form of solidarity, a mass movement"[22] werden. Dieser Konflikt wurde deutlich am Ermittlungsverfahren gegen Phil Zimmermann, bei dem sowohl Patentstreitigkeiten als auch mögliche Verletzungen der Exportrestriktionen thematisiert wurden.[23]

Beide konzeptuellen Möglichkeiten der Beschränkung von Kryptographie sollen im Rahmen der folgenden Abschnitte analysiert werden. Dazu werden wir fragen müssen, ob Exportbeschränkungen in einem globalen und vernetzten Internet sinnvoll sind, ob sie überhaupt funktionieren können und ob sie möglicherweise größeren Schaden als Nutzen anrichten. Aber auch Patentbeschränkungen sind zu diskutieren. Denn es lässt sich bereits an dieser Stelle kritisch fragen, auf welche praktische Art und Weise kryptographische Algorithmen überhaupt patentiert werden könnten, insofern sie wohl weniger Erfindung als vielmehr Entdeckung sind.[24]

Exportbeschränkungen und Patentstreitigkeiten sind aber nur zwei Möglichkeiten, mit deren Hilfe versucht wurde, die weltweite Verbreitung und ubiquitäre Anwendung von Kryptographie zu verhindern. Andere Möglichkeiten zur Regulierung von Kryptographie wären die verpflichtende Implementierung von sogenannten *Backdoors*, um Strafverfolgungsbehörden einen Zugriff auf unverschlüsselte Kommunikation zu erhalten, oder aber ein generelles Verbot der Kryptographie für Kommunikationsdienstleister.

Die Aussicht auf eine solche politische Regulierung und Beschränkung von Verschlüsselung verlieh einen entscheidenden Impuls für die Verbreitung von PGP. Der konkrete Grund war hier der *Comprehensive*

19 Siehe Levy, *Crypto*, S. 199; siehe auch Jarvis, *Crypto Wars*, S. 228–229.
20 Siehe vor allem Abschnitt 2.2.
21 ebd., S. 214.
22 Levy, *Crypto*, S. 192.
23 Siehe Jarvis, *Crypto Wars*, S. 223, allgemein auch S. 222–224.
24 Siehe dazu ebd., S. xvi. Für Jarvis ist der DH-Schlüsselaustausch eher eine Entdeckung als eine Erfindung.

Counter-Terrorism Act of 1991 (S. 266), auch genannt *Senate Bill 266*.[25] Senator Joseph R. Biden, Mitglied der Demokratischen Partei und späterer US-Präsident, schlug Anfang 1991 ein Gesetz vor, das Dienstleister und Hersteller von Kommunikationsmitteln verpflichten sollte, einen Regierungszugriff auf Klartexte von Kommunikationsdaten zu ermöglichen.[26] Somit hätte es für Unternehmen nur zwei Möglichkeiten gegeben: Entweder sie hätten keine Verschlüsselung mehr angeboten, oder sie hätten eine Backdoor implementiert, die einen Zugriff der Regierungsbehörden erlaubt hätte.[27]

Mit der Unterstützung von Kelly Goen wurde PGP daher im Jahr 1991 in die Welt hinausgesendet.[28] Wenn die Software erst einmal Abertausende von Menschen erreicht hätte, wäre sie nicht mehr zu stoppen – und nach Zimmermanns Meinung wäre dann Senate Bill 266 niemals mehr umsetzbar gewesen.[29] Was hätte die US-amerikanische Regierung dann auch tun können? Wie hätte ein solches Gesetz in der Praxis durchgesetzt werden sollen? Es ist zu bedenken, dass PGP eben keine zentralisierte Security-Software war, die einfach abgeschaltet oder reduziert werden konnte. PGP funktionierte rein auf Applikationsebene: Wer verschlüsselt per E-Mail und über das Internet kommunizieren wollte, konnte dies mit der Software von Phil Zimmermann tun. Es brauchte keine besondere Hardware, keine eigene Implementierung oder direkt steuerbare Intermediäre, die die Distribution hätten verhindern können.[30] Während PGP die Welt eroberte, zog Joe Biden den Senate Bill 266 aufgrund massiver zivilgesellschaftlicher Kritik zurück.[31]

---

25 Siehe ebd., S. 211, sowie Levy, *Crypto*, S. 195–196.

26 Siehe United States Congress. *Comprehensive Counter-Terrorism Act of 1991*. S.266. 24. Jan. 1991. URL: https://www.congress.gov/bill/102nd-congress/senate-bill/266 (besucht am 15.04.2024); auch in Levy, *Crypto*, S. 195, sowie Jarvis, *Crypto Wars*, S. 211.

27 Siehe ebd., S. 212.

28 Siehe Levy, *Crypto*, S. 197.

29 Siehe ebd., S. 197–198.

30 Auf den Aspekt der Intermediäre werden Abschnitt 4.2 und 4.3 zu sprechen kommen. Generell gilt nämlich, dass auch das Internet Intermediäre kennt, etwa Internet Service Provider (ISP). Diese können gesetzlich zu bestimmtem Handeln verpflichtet werden. Bei PGP allerdings wäre dies eine wohl nicht durchsetzbare Möglichkeit, wenn vor Inkrafttreten von Senate Bill 226 bereits Hunderttausende oder gar Millionen von Kopien existieren würden.

31 Siehe ebd., S. 198. PGP hatte zwar keinen direkten Einfluss auf den Senate Bill 266, kann aber aufgrund der ursprünglichen Motivation sowie des späteren Erfolgs durchaus als das erste große Beispiel für Cryptoaktivismus gelten.

Mit PGP war es zum ersten Mal in der Geschichte der Menschheit für Individuen möglich, digital und in großem Umfang vertraulich zu kommunizieren. Diese Entwicklung lässt sich auch im Kontext des Paradigmenwechsels verorten. Teil I hat in Anlehnung an Katz und Lindell sowie Adams drei Neuerungen der Modernen Kryptographie angesprochen:[32] Erstens wurde Kryptographie zur Wissenschaft, was seit Shannon, Diffie und anderen bereits erfüllt war. Zweitens hat Kryptographie die Sicherheit von Systemen zum Ziel – auch das ist im Kontext von Authentifizierung, Integrität und Informationssicherheit möglich geworden. Die dritte Bedingung wurde nun durch PGP realisiert: Kryptographie wird für gewöhnliche Menschen, *ordinary people*, global nutzbar, ob in Myanmar, Sarajevo oder Lettland[33] – also *überall*.[34]

Hinzu kommt, dass durch PGP eine Verschiebung von einer etwaigen Autorität hin zu mehr Dezentralität möglich wurde. Mit der Grundlage asymmetrischer Kryptographie und RSA brauchte es keine zentrale Instanz mehr, die die Schlüssel zur Ver- und Entschlüsselung verwalten musste. Im Rahmen symmetrischer Kryptographie hatte sich stets noch die Frage gestellt, wie ein geheimer Schlüssel von Alice zu Bob gelangen konnte: entweder über einen weiteren, sicheren, aber womöglich sehr unpraktikablen Kanal oder aber über eine Verwaltung und das Management von Schlüsseln, was jedoch in irgendeiner Form zentralisiert sein musste. Die Gefahr potentiellen Missbrauchs und genereller Beeinflussbarkeit war bei einer solchen zentralisierten Instanz mehr gegeben als bei einer dezentralen Lösung.[35]

Auch an einer zweiten Stelle wird deutlich, welche dezentrale Philosophie PGP verfolgen sollte. Wie Teil I gezeigt hat, ermöglicht asymmetrische Kryptographie nicht nur Vertraulichkeit, sondern mithilfe von digitalen Signaturen auch Authentizität. Doch bei digitalen Signaturen gibt es ein praktisches Problem: Zwar kann man nun feststellen, dass die gesendete Nachricht von einer Partei mit *jener* digitalen Signatur stammt. Wie aber kann man überprüfen, dass *jene* digitale Signatur auch wirklich

32 Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 3; Adams, *Introduction to Privacy Enhancing Technologies*, S. 242.

33 Siehe Greenberg, *This Machine Kills Secrets*, S. 74–75.

34 PGP ist in dieser Weise einerseits Folge der Modernen Kryptographie, andererseits aber auch Manifestation dieser Kryptographie in der Realität.

35 Zu diesen Problemen und alternativen Lösungen siehe die Diskussion in Abschnitt 2.3.

zu der *realen* Partei gehört, die sie zu sein behauptet? Im Allgemeinen handelt es sich dabei um die Frage nach der Zertifizierung von Schlüsseln und der Konstruktion sogenannter *Public-Key Infrastructures* (PKI).[36] Üblicherweise wird dazu heute ein hierarchisches Modell aus *Certification Authorities* und einer *Chain of Trust* genutzt.[37] Für Zimmermann war dies jedoch nicht umsetzbar.[38] Seine alternative Idee war, dass Drittparteien diese Schlüssel zertifizieren können.[39] Diese Drittparteien sind Entitäten, denen beide Kommunikationspartner vertrauen, wodurch ein solches Modell auch als *Web of Trust* bezeichnet wird.[40] Es handelt sich damit um eine transitive Lösung, die wiederum eine zentrale Autorität zu umgehen versucht – oder wie Levy es formuliert: „he envisioned the PGP community itself as an authority."[41]

PGP wurde damit zum singulären Ereignis für eine dezentrale, vertrauliche Organisation interpersoneller Kommunikation[42] – ein „*watershed* event"[43], wie es Zimmermann mit wohl einigem Selbstbewusstsein genannt hatte. Mit der Veröffentlichung und Distribution war PGP auch nicht mehr nur das Projekt eines Einzelnen, sondern es bildete sich eine aktive und zum Erfolg beitragende Community.[44] Um diesen Erfolg mit den treffenden Worten von Diffie und Landau zusammenzufassen:

> In writing PGP, Phil Zimmermann did something for cryptography that no technical paper could do: he gave people who were concerned with privacy but were not cryptographers (and not necessarily even programmers) a tool they could use to protect their communications.[45]

36 Siehe einführend Katz und Lindell, *Introduction to Modern Cryptography*, S. 473–479, sowie Adams, *Introduction to Privacy Enhancing Technologies*, S. 122–123; im Kontext von PGP auch Levy, *Crypto*, S. 201–203.

37 Siehe ebd., S. 201, sowie Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 548–549 und 570–572; einführend auch Anderson, *Security Engineering*, S. 194–195.

38 Siehe Levy, *Crypto*, S. 201.

39 Siehe ebd., S. 202.

40 Siehe ebd., S. 202; weiterführend auch Katz und Lindell, *Introduction to Modern Cryptography*, S. 476–477.

41 Levy, *Crypto*, S. 202.

42 Zur Singularität des Ereignisses siehe auch Jarvis, *Crypto Wars*, S. 39–41.

43 Zitiert in Levy, *Crypto*, S. 198, kursiv im Original.

44 Siehe ebd., S. 200. Zimmermann selbst war schließlich auch gar kein Kryptograph, sondern Programmierer; siehe ebd., S. 200.

45 Diffie und Landau, *Privacy on the Line*, S. 230.

Wenn PGP aber frei zugänglich geworden ist, dann bedeutet dies natürlich auch, dass nun wirklich *jede* Person die Software herunterladen und nutzen kann. Hackerinnen und Hacker, Verbrecherinnen und Verbrecher, Terroristinnen und Terroristen.[46] War damit PGP sogar eine Gefahr für die Gesellschaft und das Individuum, beispielsweise im Kontext der sogenannten Nationalen Sicherheit oder im Rahmen von Terrorismusbekämpfung? Solche Fragen sind aus ethischer Perspektive in Teil III zu diskutieren. Dabei werden wir die unterschiedlichen Facetten einer frei zugänglichen Kryptographie normativ beleuchten – vom sogenannten *Going Dark Problem* über konsequentialistische Dichotomien hin zu menschenrechtsbasierten Ansätzen. Phil Zimmermann jedenfalls hatte immer eine ganz eigene Vorstellung und Motivation:

> If privacy is outlawed, only outlaws will have privacy. [...] PGP empowers people to take their privacy into their own hands. There has been a growing social need for it. That's why I wrote it.[47]

Unabhängig von diesen ethischen und normativen Fragen wurde mit PGP eines deutlich: Wer geglaubt hatte, dass die Allgegenwart von Kryptographie und vertraulicher Kommunikation noch auf einfachem Wege zu stoppen sei, der musste spätestens mit dem Erfolg von PGP seinen Irrtum erkennen.[48] Mit Phil Zimmermann, PGP und all den weiteren Ereignissen bei der Entwicklung der Modernen Kryptographie wurde der Geist aus der Flasche gelassen, der die Kryptographie von einer rein mathematisch-technischen Wissenschaft zu einer sozial-gesellschaftlichen Frage werden ließ: *Cryptoaktivismus*.[49]

---

46 Siehe auch Levy, *Crypto*, S. 197–198.

47 Phil Zimmermann. *Why I Wrote PGP: Part of the Original 1991 PGP User's Guide (updated in 1999)*. 1999. URL: https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html (besucht am 15.04.2024); teilweise und abgewandelt zitiert auch in Levy, *Crypto*, S. 198.

48 Oder wie es Beutelspacher in seiner kurzen Einführung benennt: „PGP oder Anarchie ist machbar". Beutelspacher, *Geheimsprachen und Kryptographie*, S. 73.

49 Siehe Levy, *Crypto*, S. 205. Zu den weiteren Ereignissen siehe etwa die Diskussionen um DES, das Handeln der NSA oder die darauf folgenden juristischen Auseinandersetzungen. Weiterführend dazu Abschnitt 2.2. sowie Abschnitt 4.3.

3.2 Cryptoaktivismus

Was ist gemeint, wenn im Folgenden von *Cryptoaktivismus* gesprochen wird?[50] Im Kontext der Ethik der Kryptographie definiert diese Arbeit den Cryptoaktivismus zunächst als eine Unterkategorie eines allgemeinen *Aktivismus*. Aktivismus meint dabei eine Art von tätigem Handeln, das auf politische, soziale und gesellschaftliche Ziele fokussiert ist.[51] Eine aktivistisch handelnde Person versucht, das Ziel des Aktivismus, zum Beispiel eine gesellschaftliche Reform, *tätig* umzusetzen oder zumindest darauf hinzuwirken. Für den Cryptoaktivismus kommt nun aber hinzu, dass Kryptographie Motivation, Ziel und/oder Mittel des Aktivismus ist. Der Begriff *Crypto* bezieht sich damit in erster Linie nicht auf Kryptowährungen (engl. *Cryptocurrencies*), sondern auf *Cryptography*.[52]

Inhaltlich grenzt dieser Fokus auf Kryptographie den Cryptoaktivismus zwar von anderen Formen aktivistischen Handelns ab. Das bedeutet aber nicht, dass Cryptoaktivistinnen und -aktivisten nicht gleichzeitig auch im Bereich des Friedensaktivismus oder Umweltaktivismus oder in anderen Themenfeldern tätig sein können. Beispielsweise engagierten sich einige der ersten Cryptoaktivistinnen und -aktivisten im Rahmen der US-amerikanischen Friedensbewegung, Anti-War-Protesten und genereller *Counter Culture*.[53] Auch heute zeigt das Beispiel der einflussreichen Vereinigung des *Chaos Computer Club* (CCC), dass Cryptoaktivismus ein-

50 Bereits Levy spricht im Kontext der Cypherpunks von „cryptoactivism"; ebd., S. 205. Diese Arbeit wird im Folgenden den Begriff Cryptoaktivismus jedoch breiter fassen – über die Cypherpunks und Crypto-Anarchie hinaus. Auch Ross Anderson bezeichnet etwa Phil Zimmermann als Cryptoaktivisten; siehe Anderson, *Security Engineering*, S. 198.

51 Siehe einführend z. B. Bart Cammaerts. „Activism and media". In: *Reclaiming the Media: Communication Rights and Democratic Media Roles*.. Hrsg. von Bart Cammaerts und Nico Carpentier. Bristol: Intellect Books, 2007, S. 217–224.

52 Unglücklicherweise wird eine solche Gleichsetzung medial wie auch in der wissenschaftlichen Forschung teilweise vorgenommen. *Crypto* ist jedoch, wie die Selbstbezeichnung der Crypto-Anarchistinnen und -Anarchisten zeigt, die Abkürzung für Cryptography. Digitale Zahlmöglichkeiten sind dabei dann *eine* Unterkategorie von *Crypto*.

53 Zum Verhältnis von Cypherpunks und Counterculture siehe Jarvis, *Crypto Wars*, S. 50–54, sowie Craig Jarvis. „Cypherpunk ideology: Objectives, profiles, and influences (1992–1998)". In: *Internet Histories* 6.3 (2021), S. 315–342, hier S. 333–334. Beispielsweise war auch Zimmermann im Kontext der Friedensbewegung und von Anti-Atom-Protesten aktiv; siehe Levy, *Crypto*, S. 190, sowie Webb, *Coding Democracy*, S. 45.

gebettet ist in verschiedene und diverse gesellschaftliche Strömungen.[54] Eine Cryptoaktivistin oder ein Cryptoaktivist wird allerdings an entscheidenden Stellen der eigenen Überzeugung einen *expliziten* Bezug zur Kryptographie herstellen, sei es, um mithilfe der Kryptographie ein bestimmtes Ziel zu erreichen (etwa die Reduktion sozialer Ungerechtigkeiten), oder sei es, dass Kryptographie selbst zum Ziel wird (z. B. als grundsätzliches Recht des Menschen auf vertrauliche interpersonelle Kommunikation).

Auf eine andere Art formuliert meint dies, dass das zentrale Kriterium von Cryptoaktivismus eine *in irgendeiner Form* stattfindende Verbindung von Kryptographie und Gesellschaftlichem, Politischem oder Sozialem ist. Als Lackmustest für die Bezeichnung *Cryptoaktivismus* kann daher gelten, dass diese Art des Aktivismus bewusst einen Bezug zur Modernen Kryptographie herstellt. Cryptoaktivistinnen und -aktivisten sind fasziniert von den Prinzipien, deren Realisierung die Moderne Kryptographie ermöglicht: Privatsphäre, Dezentralität, Vertraulichkeit, Integrität, Partizipation, Transparenz. Sie entdecken in der Modernen Kryptographie eine neue Art und Weise, über Politik, Gesellschaft und Soziales nachzudenken.

Diese Arbeitsdefinition des Cryptoaktivismus ist bewusst breit gefasst. Aber gerade aufgrund dieser Unschärfe ist der Begriff für die verschiedenen Strömungen geeignet. Cryptoaktivismus umfasst nämlich mehr als das, was in Abschnitt 3.3 als *Crypto-Anarchie* und *Cypherpunks* betrachtet wird. So war etwa Phil Zimmermann kritisch gegenüber den Cypherpunks eingestellt.[55] Trotzdem ist der Einfluss von PGP auf Gesellschaft und Politik unübersehbar. Auch Zimmermanns Motive hingen stark mit den Ideen der Verschlüsselung zusammen.[56] Zimmermann war und ist nach dieser Definition also Cryptoaktivist.[57]

Cryptoaktivismus sollte in der hier vorgestellten Definition allerdings nicht mit anderen Formen des Aktivismus verwechselt werden. Eine besondere Beziehung hat er etwa zum *Hacktivismus* (engl.: *hacktivism*) –

54 Zur Einführung in die Hacker-Kultur siehe die wegweisende Arbeit Steven Levy. *Hackers: Heros of the Computer Revolution*. Ausgabe zum 25-jährigen Jubiläum. Beijing u. a.: O'Reilly, 2010; einführend zum CCC auch Webb, *Coding Democracy*, zum CCC insbesondere S. 2–5 sowie S. 13–22; siehe zudem E. Gabriella Coleman. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton und Oxford: Princeton University Press, 2013.

55 Siehe Greenberg, *This Machine Kills Secrets*, S. 85.

56 Siehe Levy, *Crypto*, S. 192.

57 Siehe auch Anderson, *Security Engineering*, S. 198.

ein Begriff, der sich aus *Hacking* und *Aktivismus* zusammensetzt.[58] Dabei muss durchaus differenziert werden. Zunächst ist der Begriff *Hacking* nicht gleichbedeutend mit Kryptographie. Sowohl gutwilliges als auch böswilliges Hacking wird zwar an bestimmten Punkten auch mit Verschlüsselung in Berührung kommen.[59] Trotzdem sind dies zwei konzeptuell verschiedene Dinge. Der Ethiker und Kommunikationswissenschaftler David J. Gunkel definiert den Begriff *Hacktivismus* wie folgt:

> "Hacktivism", as it is called, draws on the creative use of computer technology for the purposes of facilitating online protests, performing civil disobedience in cyberspace and disrupting the flow of information by deliberately intervening in the networks of global capital.[60]

Zweck und Ziel des Hacktivismus liegt also oftmals außerhalb des Hackings selbst, gerade wenn dessen Motivation etwa politischer Natur ist.[61] Hacking ist dann hauptsächlich das *Mittel* für die Umsetzung politischer Überzeugungen und weniger dessen Ziel oder gar Motivation. In der Definition des Cryptoaktivismus hingegen kann die Kryptographie ebenso gut *Motivation* wie *Ziel* sein – und ist nicht bloß Mittel zum Zweck.[62]

Cryptoaktivistinnen und -aktivisten können zudem für ihre Ziele einer freien und ubiquitären Kryptographie eintreten, ohne als Mittel auf

58 Siehe einführend Tim Jordan. *Information Politics: Liberation and Exploitation in the Digital Society*. London: Pluto Press, 2015, S. 176–191; sowie Luke Goode. „Anonymous and the Political Ethos of Hacktivism". In: *Popular Communication* 13.1 (2015), S. 74–86.

59 Sprachlich ist hier anzumerken, dass ein *Hacker* nicht per definitionem böswillig ist.

60 David J. Gunkel. „Editorial: introduction to hacking and hacktivism". In: *New Media & Society* 7.5 (2005), S. 595–597, hier S. 595.

61 Jason Andress und Steve Winterfeld definieren Hacktivismus wie folgt: „Hacktivists can be motivated by political views, cultural/religious beliefs, national pride, or terrorist ideology". Jason Andress und Steve Winterfeld. *Cyber Warfare*. 2. Aufl. Waltham: Syngress, 2014, S. 29. Zu den Motiven siehe auch George Lucas. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. New York: Oxford University Press, 2017, S. 21–22, zu staatlich gefördertem Hacktivismus ebd., S. 27–29.

62 Natürlich sind hier Grenzfälle denkbar. War beispielsweise für Tim May (siehe Abschnitt 3.3) die Kryptographie nur ein Mittel, um seine libertären Vorstellungen realisieren zu können? In jedem Fall aber soll für die Definition des Cryptoaktivismus ersichtlich werden, dass es eine enge Verbindung von Kryptographie, Mittel *und* Zielen gibt.

Kryptographie oder Hacking zurückgreifen zu müssen.[63] In der hier vorgestellten Definition des Cryptoaktivismus gibt es unterschiedliche Arten der eingesetzten Mittel, wie öffentliche Demonstrationen, politisches Engagement, Widerstand gegen legale, in der eigenen Perspektive aber illegitime Staatsgewalt oder auch juristisches Handeln. Ein sehr erfolgreiches Mittel war und ist etwa, auf die logische Widersprüchlichkeit und die Irrationalitäten von Gesetzen oder Regulierungen hinzuweisen.[64] Allerdings bleibt dabei der Einsatz von Kryptographie – also von vertraulicher, integrer und authentifizierter Kommunikation – *ein weiteres* Mittel zur Erreichung der jeweiligen Ziele.

Trotz dieser konzeptuellen Unterschiede von Hacktivismus und Cryptoaktivismus sind die Grenzen je nach Definition fließend. So erkennt etwa Tim Jordan zwei verschiedene Kulturen des Hacktivismus:

> These are two key cultures for hacktivism that had come into existence by the early 1990s: breaking into computer networks as a form of intellectual exploration, intellectual because cracking was primarily through expertise rather than hardware; and the rise of an ideology conceiving of computer networks as creating a place with its own politics, primarily that of freedom of information.[65]

Gerade diese zweite Kultur eines Ortes mit eigener Politik und Informationsfreiheit ist auf parallele Weise auch im Bereich des Cryptoaktivismus erkennbar. Deutlich wird dies vor allem an den Diskussionen in Abschnitt 4.1, der sich mit dem Verhältnis des *Cyberspace*, Internet und Kryptographie auseinandersetzen wird. Eine genaue Abgrenzung ist daher nicht immer möglich. Meist ist Cryptoaktivismus allerdings mit folgender Charakterisierung differenzierbar: Cryptoaktivismus ist bezüglich Kryptographie als Motivation und Ziel spezifischer und expliziter, als dies andere Formen des Aktivismus sind. Was die Mittel zur Erreichung der Ziele angeht, ist Cryptoaktivismus jedoch flexibel und verlässt sich nicht allein auf die Kryptographie.

---

63 Aus ähnlichen Gründen ist Cryptoaktivismus nicht gleichzusetzen mit *Cyber-Aktivismus* oder *Internet-Aktivismus*.

64 Beispielhaft ist das Wirken von Phil Karn zu nennen, das in Abschnitt 4.3 im Kontext von Exportbeschränkungen diskutiert werden wird. Weiter unten sind zudem der juristische Fall um Daniel Bernstein sowie das zivilgesellschaftliche Engagement der *Electronic Frontier Foundation* zu betrachten.

65 Jordan, *Information Politics*, S. 184.

Motivation und Ziel sind also an irgendeiner Stelle mit dem Gedanken der Kryptographie verbunden. Doch das bedeutet nicht, dass alle Cryptoaktivistinnen und -aktivisten gleiche politische Ansichten hätten. Zum Beispiel scheint der Cryptoaktivismus in den USA historisch betrachtet oft anarcho-libertär beeinflusst.[66] In Europa hingegen zeigt sich mit Blick auf zentrale Vereinigungen der Szene (z. B. den *Chaos Computer Club*) eine eher sozial-gesellschaftliche und linksgerichtete Orientierung. Auch hier sind trennscharfe Unterscheidungen daher nicht immer möglich. Als weitere politische Gemeinsamkeit neben der Idee der Kryptographie kann jedoch definiert werden, dass mit Cryptoaktivismus auffallend oft eine Ablehnung von Autorität einhergeht.

Durch diese Unschärfe in der politischen Ausrichtung und infolge der antiautoritären Haltung gibt es auch keine *zentrale* Person oder Instanz, die als für den Cryptoaktivismus verantwortlich gelten kann. Vielmehr zeigt sich im Cryptoaktivismus ein starker *Bottom-up*-Ansatz: Es handelt sich um eine Bewegung *von unten*, die zunächst vom Individuum und seinem Wirkungsbereich ausgeht.[67] Ein Individuum kann, wenn es zum Erreichen seiner Ziele etwa Kenntnisse aus der Kryptographie oder Programmierung nutzt, bereits *allein* oder in kleinen, dezentralen Gruppen eine große Wirkung erzielen.[68] Mit Phil Zimmermann ist ein Beispiel diskutiert worden, bei dem eine einzelne Person eine Software schreiben konnte, die den Diskurs und die Gesellschaft über Jahrzehnte zu beeinflussen vermochte.[69] Ein anderes Beispiel ist im Kontext des sogenannten *Escrowed Encryption Standard* (respektive *Clipper-Chip*) zu nennen. Dieser Standard war ein Versuch der US-amerikanischen Regierung gewesen, Zugriff auf kryptographische Schlüssel zur Entschlüsselung zu erhalten.[70] Der Kryptograph Matt Blaze konnte jedoch als einzelnes Individuum und mit geringem Aufwand zeigen, dass dieser Chip entscheidende Schwachstellen aufwies.[71]

66 Insbesondere durch die Cypherpunks und die Crypto-Anarchie.

67 Beispielsweise war für Levy Zimmermanns PGP ein „bottom-up crypto phenomenon". Levy, *Crypto*, S. 204.

68 Dies stellt somit eine Gemeinsamkeit mit dem Hacktivismus dar.

69 Anschließend hat sich zwar rasch eine Community um PGP gebildet, den Anstoß dazu ermöglichte aber Phil Zimmermann. Siehe ebd., S. 200.

70 Siehe dazu Abschnitt 4.3; einführend außerdem Diffie und Landau, *Privacy on the Line*, S. 234–248, sowie Rid, *Rise of the Machines*, S. 273–276.

71 Siehe Matt Blaze. „Protocol Failure in the Escrowed Encryption Standard". In: *Proceedings of the 2nd ACM Conference on Computer and Communications Security*.

Trotz dieser individuellen Möglichkeiten können sich Cryptoaktivistinnen und -aktivisten in Gruppierungen und Institutionen organisieren. Die wohl bekannteste und erfolgreichste Organisation dieser Art dürfte die *Electronic Frontier Foundation* sein, die wohl zu Recht als intellektuelle und politische Heimat für den Cryptoaktivismus gelten kann.[72] Noch vor dem ersten Treffen der sogenannten Cypherpunks, die Abschnitt 3.3 diskutieren wird, gründeten John Perry Barlow, Mitch Kapor und John Gilmore im Jahr 1990 die Organisation mit der Abkürzung *EFF*.[73] Gilmore legte ein Jahr später auf einer Konferenz seine Utopie über eine Gesellschaft von morgen dar:

> What if we could build a society where the information was never collected? Where you could pay to rent a video without leaving a credit card or bank account number? Where you could prove you're certified to drive without giving your name? Where you could send and receive messages without revealing your physical location, like an electronic post office box? That's the kind of society I want to build. I want to guarantee – with physics and mathematics, not with laws – things like real privacy of personal communication [...].[74]

Hier zeigt sich bereits, wie Cryptoaktivismus oft aus einer starken natur- und technikwissenschaftlichen Perspektive argumentiert. Es seien eben nicht die Gesetze oder Regulierungen, die uns Sicherheit, Privatsphäre und Freiheit ermöglichen. In der Zukunft würden es – durch die Kryptographie – die Gesetze der Mathematik und der Physik sein, die die Gesellschaft zum Besseren werden lassen. Es handelt sich hier also auch um eine Art Determinismus, insofern die Gesetze der Mathematik keine Regierung dieser Welt, kein noch so reiches Unternehmen verändern könnte. Die Moderne Kryptographie wird hier verbunden mit dem Narrativ einer gesellschaftlichen und politischen Neuausrichtung, die damit das zentrale Kriterium eines Cryptoaktivismus erfüllt.

Fairfax, Virginia. CCS '94. Association for Computing Machinery, 1994, S. 59–67; einführend auch Jarvis, *Crypto Wars*, S. 187.

72 Jeff Moss bezeichnete die EFF einmal als „the closest thing hackers have to a religion"; zitiert nach ebd., S. 212.

73 Siehe ebd., S. 212. Gilmore war dabei auch ein früher Aktivist der Cypherpunks. Siehe einführend auch Webb, *Coding Democracy*, S. 40–44.

74 Zitiert nach Levy, *Crypto*, S. 208.

Diese Vorstellung wird auch deutlich an John Perry Barlow, der vielleicht bekanntesten Figur der EFF.[75] Am 7. Februar 1996 publizierte er seine *Unabhängigkeitserklärung des Cyberspace* (engl. *A Declaration of the Independence of Cyberspace*), die Craig Jarvis auch als „[o]ne of the best reflections of the hacker and cypherpunk philosophy" bezeichnet.[76] Das Datum war aber nicht irgendein Datum: Zeitgleich fand in Davos das *Weltwirtschaftsforum* (WEF) statt, von dem aus er seine Erklärung veröffentlichte.[77] In seiner Erklärung spricht er direkt die Regierungen der industriellen Welt an, die er als „weary giants of flesh and steel"[78] bezeichnet. Er stellt bereits im ersten Absatz eine trennscharfe Dichotomie zwischen Regierungen und Staaten einerseits und dem Cyberspace andererseits dar. Unmissverständlich macht er deutlich, dass Regierungen und Staatsangelegenheiten im Cyberspace nicht willkommen seien.

Barlow vertrat dabei sicherlich eine provokant-prosaische Utopie. Die EFF jedoch, die er mitbegründet hatte, entwickelte sich in den Folgejahren zu einer überaus erfolgreichen und zivilgesellschaftlichen Organisation, die ein breites Spektrum an Themen abdecken sollte.[79] An der EFF wird daher auch pointiert deutlich, wie Technologie und Gesellschaft im Kontext von Kryptographie zusammenwirken. Um ihre Ziele zu erreichen, engagiert sich die EFF einerseits mit technologisch-praktischen Entwicklungen. Einflussreich war hier etwa der sogenannte *DES Cracker* aus dem Jahr 1998.[80] Mit diesem konnte die EFF kostengünstig in der

75 John Perry Barlow war denn auch Songtexter der bekannten Band *Grateful Dead*. Siehe zu Barlow einführend Greenberg, *This Machine Kills Secrets*, S. 254–255, sowie Rid, *Rise of the Machines*, S. 224–227.

76 Jarvis, *Crypto Wars*, S. 49, allgemeiner auch S. 49–50.

77 Siehe dazu die Signatur der Erklärung: John Perry Barlow. *A Declaration of the Independence of Cyberspace*. Davos, 8. Feb. 1996. URL: https://www.eff.org/de/cyberspace-independence (besucht am 15.04.2024); weiterführend Rid, *Rise of the Machines*, S. 244–245; zum Kontext auch Webb, *Coding Democracy*, S. 48–51.

78 Barlow, *A Declaration of the Independence of Cyberspace*; zum Folgenden ebd.

79 Wie etwa Redefreiheit, Transparenz, Sicherheit, Privacy und andere Themen im Kontext von Digitalisierung und Grundrechten. Siehe dazu etwa den jährlichen Bericht: Electronic Frontier Foundation. *EFF's 2021 Annual Report*. 2021. URL: https://www.eff.org/files/2023/10/03/eff_2021_annual_report_final.pdf (besucht am 15.04.2024).

80 Siehe dazu und zum Folgenden Electronic Frontier Foundation. *"EFF DES Cracker" Machine Brings Honesty to Crypto Debate: EFF Builds DES Cracker that proves that Data Encryption Standard is insecure*. 17. Juli 1998. URL: https://web.archive.org/web/19990202034950/http://www2.eff.org/pub/Privacy/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html (besucht am 15.04.2024).

Praxis nachweisen, dass der Data Encryption Standard (DES) innerhalb weniger Tage gebrochen werden kann.[81] Für John Gilmore bedeutete das:

> Now that the public knows, it will not be fooled into buying products that promise real privacy but only deliver DES. This will prevent manufacturers from buckling under government pressure to "dumb down" their products, since such products will no longer sell.[82]

Neben technologisch-praktischer Entwicklungen betätigt sich die EFF andererseits aber auch gesellschaftlich, politisch und juristisch. Eines der ersten Ereignisse, das bedeutend für den Umgang mit Kryptographie werden sollte, war der Fall *Bernstein v. US Department of Justice*: Daniel Bernstein, damaliger Doktorand an der UC Berkeley, war in den 1990er-Jahre aufgrund von Exportbeschränkungen kryptographischer Algorithmen in eine Auseinandersetzung mit der US-amerikanischen Regierung geraten.[83] Daraufhin unterstützte die EFF Bernstein ab 1995 juristisch.[84] In der Konsequenz führte unter anderem diese Auseinandersetzung dazu, dass Kryptographie als ein Ausdruck der freien Meinungsäußerung anerkannt wurde.[85] Zum 25. Geburtstag der EFF fasste Alison Dame-Boyle den Erfolg von *code is speech* wie folgt zusammen:

> Today it may seem obvious that communication using programming languages is protected by the First Amendment. But before this decision, no judge had formalized that principle in a ruling. *Bernstein* helped pave the way for the growing use of encryption that makes web browsing and activities like banking and shopping more secure, and its recognition of code as speech helped build the legal foundation for online rights being recognized alongside offline ones.[86]

81 Gebrochen worden war DES durch die DES Challenge *DESCHALL* zwar schon 1997. Dies erforderte jedoch zahlreiche Freiwillige, die ihre Rechenleistung zur Verfügung gestellt hatten. Siehe einführend zu *DESCHALL* Jarvis, *Crypto Wars*, S. 95–97.

82 Zitiert in Electronic Frontier Foundation, *„EFF DES Cracker" Machine Brings Honesty to Crypto Debate*.

83 Siehe Jarvis, *Crypto Wars*, S. 238–257, sowie Alison Dame-Boyle. *EFF at 25: Remembering the Case that Established Code as Speech*. Electronic Frontier Foundation. 16. Apr. 2015. URL: https://www.eff.org/de/deeplinks/2015/04/remembering-case-established-code-speech (besucht am 15.04.2024). Siehe auch Abschnitt 4.3.

84 Siehe Jarvis, *Crypto Wars*, S. 243. Die EFF engagierte sich andererseits auch im Fall Phil Zimmermanns und *Pretty Good Privacy*; siehe ebd., S. 223.

85 Siehe ebd., S. 257.

86 Dame-Boyle, *EFF at 25*, kursiv im Original.

Was bedeutet solcher Cryptoaktivismus aber letztlich im Kontext der Ethik der Kryptographie? Die zugrundeliegende These von Teil II ist, dass Moderne Kryptographie nicht nur Technologie oder Mathematik ist, sondern eben auch eine genuin sozial-gesellschaftliche Angelegenheit. Der Cryptoaktivismus, wie er in Form der EFF oder im Wirken einzelner Individuen in Erscheinung tritt, zeigt diese enge Verflechtung von Technologie und Gesellschaft. Eine Systematisierung des Cryptoaktivismus bleibt zwar aufgrund pluraler und diverser Einzelpersonen, Organisationen und Strömungen unscharf und herausfordernd. Gerade deswegen lohnt es sich jedoch, den Cryptoaktivismus an einer weiteren, womöglich seiner radikalsten Strömung überhaupt zu verdeutlichen: den Cypherpunks und der Idee einer Crypto-Anarchie.[87]

3.3 Cypherpunks und Crypto-Anarchie

Am 19. September 1992 traf sich eine ausgewählte Gruppe bestehend aus ungefähr zwanzig Personen zum ersten Mal im Rahmen eines persönlichen Meetings in Berkeley, USA.[88] Der Name der Gruppe lautete bis dahin *Cryptology Amateurs for Social Irresponsibility*.[89] Das Treffen wurde zur Geburtsstunde der sogenannten *Cypherpunks*. Die spätere Selbstbezeichnung entstand dabei durch eine Abwandlung des Begriffs *Cyberpunk*: Der Teil *Cyber* wurde ersetzt durch den Begriff *Cypher*, also eine Mischung aus *Cipher* und *Cyber*.[90] Dreißig Jahre später definieren Ramiro und de Queiroz die Cypherpunks wie folgt:

> *Cypherpunk* refers to social movements, individuals, institutions, technologies, and political actions that, with a decentralised approach, defend, support, offer, code, or rely on strong encryption systems in order to reshape social, political, or economic asymmetries.[91]

87 Manche dieser Ansichten sind bereits in den vorherigen Abschnitten angeklungen, beispielsweise bei John Perry Barlow und seiner *Unabhängigkeitserklärung des Cyberspace*.

88 Siehe Levy, *Crypto*, S. 209.

89 Siehe ebd., S. 209; einführend auch Jarvis, *Crypto Wars*, S. 30–33.

90 Siehe Levy, *Crypto*, S. 211.

91 André Ramiro und Ruy de Queiroz. „Cypherpunk". In: *Internet Policy Review* 11.2 (2022), S. 2, kursiv im Original. Eine weitere Definition stammt von Craig Jarvis. Für ihn waren die Cypherpunks „a highly educated, mostly libertarian community permea-

Einer, der als Mitgründer von Anfang an dabei war, war Timothy C. May.[92] May gilt wohl zu Recht als einer der bekanntesten, sicherlich aber auch provokantesten Cypherpunks der frühen Jahre.[93] Er hatte bereits wenige Jahre zuvor einen kurzen Text mit dem Titel *The Crypto Anarchist Manifesto* verfasst, in dem er seine Vorstellung einer neuen, auf dem Fundament der Kryptographie aufgebauten Gesellschaft erläutert.[94] Er schreibt darin von anonymer Kommunikation, auch davon, dass Staaten versuchen würden, diese Entwicklung zu stoppen, und betont, dass nichts die Crypto-Anarchie aufhalten könne:

> The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.[95]

Anschließend zieht er eine analogische Parallele zum Mittelalter und zum Buchdruck, womit er den für ihn besonderen Status der Kryptographie verdeutlicht:

> Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamen-

---

ted by aspects of anarchism which arose from a societal disaffiliation inherited from the counterculture", die zudem beeinflusst waren durch die Hackerethik und dystopische Science-Fiction; Jarvis, „Cypherpunk ideology", S. 315. Siehe zu den Cypherpunks auch Rid, *Rise of the Machines*, S. 246–293. Eine kritische, teils überaus polemische Auseinandersetzung mit den Cypherpunks findet sich bei Paulina Borsook. *Cyberselfish: A Critical Romp through the Terribly Libertarian Culture of High Tech*. New York: PublicAffairs, 2000, insbesondere S. 73–114. Zu einer Selbstbeschreibung der späteren Generation der Cypherpunks siehe vor allem Assange u. a., *Cypherpunks*.

92 Siehe einführend zu May Levy, *Crypto*, S. 206, sowie Rid, *Rise of the Machines*, S. 258–261; zudem Webb, *Coding Democracy*, S. 34–39.

93 Jacob Appelbaum charakterisierte May z. B. als „fucking racist"; zitiert in Greenberg, *This Machine Kills Secrets*, S. 92.

94 Siehe Timothy C. May. *The Crypto Anarchist Manifesto*. 1988. URL: https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html (besucht am 15.04.2024).

95 Ebd.

> tally alter the nature of corporations and of government interference in economic transactions.[96]

Damit entwickelte May die ideologische Grundlage der *Crypto-Anarchie*.[97] Der Journalist Jamie Bartlett bezeichnet die Crypto-Anarchie gar als „one of the very few genuinely original – and utterly revolutionary – political philosophies of the last 50 years"[98]. Auch einige der Cypherpunks standen der Idee einer solch radikalen, neuen Philosophie nahe.[99] May selbst war zudem, wie viele der Cypherpunks, stark libertär geprägt.[100] Nach eigener Aussage waren es die Werke von Ayn Rand, die ihn noch in jungen Jahren zu konvertieren vermochten.[101] Seine politische Philosophie sollte er später wie folgt beschreiben: „My political philosophy is keep your hands off my stuff. Out of my files, out of my office, off what I eat, drink, and smoke. If people want to overdose, c'est la vie. Schadenfreude."[102]

Eine weitere Quelle, welche die Ideen und Ziele der Cypherpunks pointiert beschreiben kann, ist Mays *Cyphernomicon*, eine Art inoffizieller *Frequently Asked Questions* (FAQ) über die Cypherpunks.[103] Er betont darin zwar, dass dies keine offiziellen FAQ der Cypherpunks seien. Als eine lose, dezentrale und diverse Gruppierung wären solche wohl auch nicht möglich. Trotzdem wird an kaum einem Dokument so umfassend deutlich, welche Art von *Denkweise* die Cypherpunks im Kontext von

96 Ebd.

97 Nach Jarvis war er „crypto-anarchy's ideological founder". Jarvis, *Crypto Wars*, S. 28. Siehe zu einer aktuellen und kritischen Einführung in die Crypto-Anarchie auch Jamie Bartlett. *The People Vs Tech: How the internet is killing democracy (and how we save it)*. London: Ebury Press, 2018, S. 161–189. Bartlett schreibt darin zudem vom Prager *Paralelní Polis* und dem *Institute of Cryptoanarchy*, wo inzwischen viele Veranstaltungen zu Themen wie etwa Dezentralität, Kryptowährungen, Crypto-Anarchie oder Privatsphäre stattfinden. Siehe zur umfassenden Einführung, insbesondere im Kontext der Kybernetik, auch Rid, *Rise of the Machines*, S. 246–293.

98 Bartlett, *The People Vs Tech*, S. 162.

99 Siehe Levy, *Crypto*, S. 211. Die von May entwickelte Ideologie war nach Ansicht von Craig Jarvis zudem „broadly, though not entirely, representative of the cypherpunk community." Jarvis, „Cypherpunk ideology", S. 315.

100 Siehe Levy, *Crypto*, S. 206. Zur Zusammensetzung der Cypherpunks siehe weiter unten.

101 Siehe ebd., S. 206.

102 Zitiert nach Greenberg, *This Machine Kills Secrets*, S. 58.

103 Siehe Timothy C. May. *The Cyphernomicon*. 1994. URL: https://nakamotoinstitute.org/static/docs/cyphernomicon.txt (besucht am 15.04.2024).

Kryptographie und Gesellschaft haben konnten. Der Politikwissenschaftler Thomas Rid bezeichnet das Cyphernomicon daher auch als „perhaps the closest thing the movement has to a canonical document“[104]. May beantwortet darin etwa auch die Frage, wie er all diese Ideen mit der Demokratie vereinen möchte:

> I don't; democracy has run amok, fulfilling de Tocqueville's prediction that American democracy would last only until Americans discovered they could pick the pockets of their neighbors at the ballot box.[105]

Auch in diesen Texten ist die libertäre Ausrichtung Mays unverkennbar. Seiner Meinung nach war auch etwa die Hälfte der frühen Cypherpunks libertär-anarchistisch, 20 Prozent waren dagegen liberal oder links, und die politische Einstellung der übrigen 20 Prozent war nicht bekannt.[106] Neben May gelten John Gilmore und Eric Hughes als libertäre Mitgründer der Cypherpunks.[107] Steven Levy erkennt zwar an, dass Hughes' Vision im Vergleich zu May verblasste, denn Mays Gedanken über Kryptographie seien „almost like dropping acid“[108]. Trotzdem verfolgte auch Hughes eine libertäre Agenda, die Levy wie folgt beschreibt:

> His ultimate goal was combining pure-market capitalism and freedom fighting. In his world view, governments – even allegedly benign ones like the United States – were a constant threat to the well-being of citizens. Individual privacy was a citadel constantly under attack by the state. The great miracle was that the state could be thwarted by algorithms.[109]

104 Rid, *Rise of the Machines*, S. 265.

105 May, *The Cyphernomicon*. May ging auch, im Unterschied beispielsweise zu Assange, davon aus, dass Kryptographie den *Übermenschen* Nietzsches befähigen werde, nicht die Mehrheit der Menschen. Siehe Rid, *Rise of the Machines*, S. 291–292; dazu auch Bartlett, *The People Vs Tech*, S. 189.

106 Siehe Jarvis, *Crypto Wars*, S. 5. Paulina Borsook charakterisiert die Cypherpunks auch wie folgt: „In cypherpunk cyberpunk dreams, everything consensual/contractual/privatized ensues (any two individuals can arrange anything they want among themselves with no busybody intrusion of third parties such as government or fellow feeling), although chaos, improvidently, is loosed upon most.“ Borsook, *Cyberselfish*, S. 18.

107 Siehe Levy, *Crypto*, S. 209. Siehe zu Hughes auch Greenberg, *This Machine Kills Secrets*, S. 78, sowie Rid, *Rise of the Machines*, S. 261–262, zu Gilmore S. 269–271.

108 Levy, *Crypto*, S. 207.

109 Ebd., S. 206.

Obgleich politische Gemeinsamkeiten bei den Cypherpunks erkennbar sind, unterscheiden sich ihre Vorstellung in der prozeduralen Umsetzung teils erheblich. Insbesondere in der Radikalität, mit der die ein oder andere Form der Crypto-Anarchie umgesetzt werden sollte, gab es unterschiedliche Meinungen. Eine der provokantesten Ideen war dabei die sogenannte *Assasination Politics*.[110] Craig Jarvis beschreibt sie auch als die „most extreme Crypto-Anarchist manifestation"[111]. Auch wenn sie nie umgesetzt wurde, zeigt die Auseinandersetzung mit einer solchen Idee einerseits, welche Radikalität vereinzelte Cypherpunks verfolgten. Andererseits wird an kaum einem anderen Beispiel so deutlich, wie sehr sich Kryptographie auf das Verhältnis von Technologie, Gesellschaft und Ethik auswirkt. Die *Assasination Politics* wird zur Raison d'Être einer Ethik der Kryptographie.

Jim Bell veröffentlichte im Jahr 1996 einen zehnteiligen Essay mit dem Titel *Assasination Politics*.[112] Er selbst beschreibt darin seine Theorie als eine „quite literally 'revolutionary' idea"[113], die er „jokingly"[114] als Assasination Politics bezeichnet. Der Journalist Andy Greenberg schreibt in diesem Zusammenhang über Bell:

> Like May, he was a libertarian to his core. And for both men, in their own ways, the advent of anonymous messaging and anonymous payments represented not just the possibility, but the inevitability of crypto-anarchy. Bell's path to that end was just a bit bloodier.[115]

Bells Assasination Politics funktioniert in etwa wie folgt: Es soll eine Organisation geben, die ein Preisgeld an denjenigen vergibt, der den Tod einer bestimmten, gelisteten Person korrekt *vorhersagt*.[116] Jene Person muss auf einer Liste von Personen stehen, die das libertäre *Non-Agression Prin-*

110 Siehe Jim Bell. *Assasination Politics*. 3. Apr. 1997. URL: https://cryptome.org/ap.htm (besucht am 15.04.2024).

111 Jarvis, *Crypto Wars*, S. 25.

112 Siehe Bell, *Assasination Politics*; einführend zu Bell und der Assasination Politics Jarvis, *Crypto Wars*, S. 25–29, sowie Rid, *Rise of the Machines*, S. 281–284.

113 Bell, *Assasination Politics*.

114 Ebd.

115 Greenberg, *This Machine Kills Secrets*, S. 119.

116 Siehe dazu und zum Folgenden Bell, *Assasination Politics*. Im Original ist *vorhergesagt* in Anführungszeichen gesetzt. Einführend auch Jarvis, *Crypto Wars*, S. 25–29, sowie Greenberg, *This Machine Kills Secrets*, S. 119–122.

ciple verletzten, etwa Regierungsmitarbeitende. Jeder Person auf dieser Liste wird zudem ein monetärer Wert als Preisgeld zugeordnet. Durch die Kryptographie und die Möglichkeit anonymer, digitaler Transaktionen wären Beiträge und Wetten möglich, ohne dass die Identität des Wettenden bekannt werden müsste. Doch nur eine wettende Person wüsste den exakten Zeitpunkt des Todes und würde damit das gesammelte Preisgeld erhalten: die Mörderin bzw. der Mörder.[117]

Im Allgemeinen handelt es sich damit also um ein System, das die Risiken der Mörderin bzw. des Mörders reduzieren und Anreize schaffen soll, Personen auf dieser Liste zu töten – mithilfe von Public-Key-Kryptographie, anonymen Relays und Kryptowährungen.[118] Jim Bell schreibt über die scheinbaren Vorteile:

> Consider how history might have changed if we'd been able to "bump off" Lenin, Stalin, Hitler, Mussolini, Tojo, Kim Il Sung, Ho Chi Minh, Ayatollah Khomeini, Saddam Hussein, Moammar Khadafi, and various others, along with all of their replacements if necessary, all for a measly few million dollars, rather than the billions of dollars and millions of lives that subsequent wars cost.[119]

Worauf eine solch radikale Vorstellung im Kontext der Ethik der Kryptographie hinweisen soll, ist die Tragweite, mit der Kryptographie und Gesellschaft gedanklich verbunden werden kann. Die Moderne Kryptographie ist eben nicht mehr nur reine Technologie. Moderne Kryptographie ist Voraussetzung für und Beginn der verschiedensten, provokantesten und radikalsten Vorstellungen über Gesellschaft und Politik. Aufgrund dieser neuartigen und unterschiedlichen Positionen ist auch eine normativ-wissenschaftliche Untersuchung, wie sie in Teil III vorgenommen wird, relevant und notwendig.

Betont werden muss zur Assasination Politics jedoch auch, dass sie nicht für die allgemeine Cypherpunk-Bewegung oder generell für den Cryptoaktivismus stehen kann – die Idee der Assasination Politics wurde auch von zahlreichen Mitgliedern der Cypherpunks scharf kritisiert.[120] Sogar Tim May war ablehnend gegenüber Bells Idee eingestellt, obgleich

117 Siehe Greenberg, *This Machine Kills Secrets*, S. 120.
118 Siehe Jarvis, *Crypto Wars*, S. 26.
119 Bell, *Assasination Politics*.
120 Siehe Greenberg, *This Machine Kills Secrets*, S. 121–122.

wohl eher aus opportunistischen Gründen.[121] Ebenso wies Phil Zimmermann die Assasination Politics entschieden zurück.[122]

Trotz dieser Differenzen in der prozeduralen Radikalität verbindet die meisten Cypherpunks eine in der ein oder anderen Form systemkritische, freiheitliche und antiautoritäre Haltung.[123] Einerseits war dies sicherlich dadurch bedingt, dass auch das frühe Internet durch freiheitliche Vorstellungen geprägt war.[124] Die Möglichkeit, eine parallele, digitale, sich selbst die Normen gebende Erfahrungswelt zu erschaffen und zu gestalten, ist für freiheitsorientierte Personen und Gruppierungen attraktiv. Andererseits liegt dies inhaltlich auch der Modernen Kryptographie nahe, insofern sie Anonymität, Dezentralität und Privacy realisieren soll.

Eine andere Homogenität der Gruppierung wird mit Blick auf die beruflichen Hintergründe deutlich. May war zum Beispiel trotz seiner ausgeprägten politischen Ansichten kein universitär ausgebildeter Philosoph oder Staatstheoretiker, sondern Physiker.[125] Wie Jarvis erkennt, waren auch viele der anderen Cypherpunks „eminent physicists, computer scientists, and academics – they were the intellectual elite with legitimate concerns based on a history littered with serious government abuses of privacy“[126]. Mit der Kryptographie als dem zentralen Element der Cypherpunk-Philosophie mag es kaum überraschen, dass viele Cryptoaktivistinnen und -aktivisten gerade in den frühen Jahren einen technischen, mathematischen oder naturwissenschaftlichen Hintergrund hatten. Um die Bedeutung der Modernen Kryptographie zu erfassen, war sicherlich ein basales Verständnis ihrer Grundlagen erforderlich. Zusammenfassend handelt es sich daher bei den Cypherpunks zwar einerseits um eine heterogene Gruppierung, was die Einordnung, Radikalität und Umsetzung der politischen Ideen betraf. Andererseits verbindet die Cypherpunks

121 Siehe Jarvis, *Crypto Wars*, S. 28–29; dazu auch Greenberg, *This Machine Kills Secrets*, S. 121–122.

122 Siehe ebd., S. 122; auch genannt in Jarvis, *Crypto Wars*, S. 29.

123 Siehe umfassender zu den Vorstellungen der Cypherpunks Enrico Beltramini. „Against technocratic authoritarianism: A short intellectual history of the cypherpunk movement“. In: *Internet Histories* 5.2 (2021), S. 101–118, zur antiautoritären Haltung S. 113.

124 Siehe dazu Abschnitt 4.1.

125 Siehe Levy, *Crypto*, S. 206.

126 Jarvis, *Crypto Wars*, S. 41. Beim Cypherpunk-Treffen am 19. September 1992 waren allerdings auch ein paar *Extropians* anwesend; siehe Levy, *Crypto*, S. 209.

aber das mathematisch-naturwissenschaftliche Interesse an der Modernen Kryptographie.

An erster Stelle steht für die Cypherpunk-Philosophie daher auch nicht die akademische oder publizistische Beschäftigung mit Politik und Philosophie, sondern das von Eric Hughes geprägte aktivistische Mantra: „Cypherpunks write code“ [127]. Wie er in *A Cypherpunk's Manifesto* schreibt, spielt es für die Cypherpunks keine Rolle, ob diesem Code zugestimmt werde oder nicht. [128] Seine Überzeugung formuliert er mit einigem Selbstbewusstsein, denn für ihn ist klar: „We know that software can't be destroyed and that a widely dispersed system can't be shut down.“ [129]

Letztlich geht es bei all dem um die Frage, was Software im Eigentlichen ist. Für die Cypherpunks jedenfalls nicht mehr (und nicht weniger) als Information, die nicht aufzuhalten ist. Zwanzig Jahre später war Hughes im Rückblick auf seine damalige Überzeugung allerdings weitaus selbstkritischer. In einem Interview mit der deutschen Wochenzeitung *Die ZEIT* antwortete er auf die Frage, was er heute anders machen würde, wenn er erneut eine politische Bewegung für ein freies Internet gründen wollen würde:

> … und ich sage noch mal ausdrücklich: Das tue ich nicht! Aber theoretisch gesprochen würde ich heute ein politisches Netzwerk zur Unterstützung bauen, bevor ich viel Zeit mit dem Programmieren verbrächte. Ich würde Leute suchen, die im politischen Lobbying Erfahrungen haben, denn wir müssten Menschen für unsere Themen begeistern, über die klassischen Parteigrenzen hinweg. [130]

Aber auch wenn Hughes heute eine differenziertere Perspektive zum Mantra *Cypherpunks write code* vertritt, ist überraschend, wie erfolgreich die Ideale der Cypherpunks umgesetzt wurden. Das vorherige Kapitel hat bereits PGP als eine Instanz für Software besprochen, die nicht gestoppt werden zu können scheint. Andererseits kann als Beispiel auch

127 Eric Hughes. *A Cypherpunk's Manifesto*. 1993. URL: https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt (besucht am 15.04.2024). Siehe auch Greenberg, *This Machine Kills Secrets*, S. 82, sowie Jarvis, *Crypto Wars*, S. 38–39, und Rid, *Rise of the Machines*, S. 271–272.

128 Siehe dazu und zum Folgenden Hughes, *A Cypherpunk's Manifesto*.

129 Ebd.

130 Interview in Thomas Fischermann. „Der Überwachungsalptraum ist wahr geworden“. In: *ZEIT Online* (20. Sep. 2013). URL: https://www.zeit.de/digital/internet/2013-09/cypherpunks-eric-hughes/komplettansicht (besucht am 15.04.2024).

die Entwicklung der Whistleblowing-Plattform *Wikileaks* gelten, die einer der wohl bekanntesten Cypherpunks aller Zeiten gegründet hat: Julian Assange.[131] Für ihn sollte die Entwicklung von kryptographischen Tools nicht allein in den Händen der Regierungen liegen:

> The notion is that you cannot trust a government to implement the policies that it says it is implementing, and so we must provide the underlying tools, cryptographic tools that we can control, as a sort of use of force, in that if the ciphers are good no matter how hard it tries a government cannot break into your communications directly.[132]

Aber auch an einer weiteren Idee wird der heutige Einfluss von *Cypherpunks write code* deutlich: an anonymen, digitalen Bezahlmöglichkeiten. Die Faszination anonymer Zahlungen trieb auch den Kryptographen David Chaum an, einen späteren Professor an der New York University und der University of California.[133] Levy beschreibt Chaum als „bearded, ponytailed, Birkenstocked cryptographer and businessman"[134], der „arguably the ultimate cypherpunk"[135] gewesen sei, indem er die mathematische und philosophische Basis für die Cypherpunk-Bewegung geschaffen habe.[136] Mit den kryptographischen Methoden, die er entwickelt hatte, wurde er zum „Houdini of crypto"[137], denn er konnte bereits in den 1980ern zeigen: Anonyme Finanztransaktionen sind kryptographisch möglich.[138] Auch an Chaum wird damit ersichtlich, wie eng Kryptographie, Gesellschaft und nun auch Wirtschaft zusammenhängen.[139]

131 Siehe zu Wikileaks einführend Webb, *Coding Democracy*, S. 56–60.

132 Assange u. a., *Cypherpunks*, S. 60–61.

133 Siehe zur Biographie Chaums Greenberg, *This Machine Kills Secrets*, S. 65–66; einführend auch Rid, *Rise of the Machines*, S. 256–258.

134 Levy, *Crypto*, S. 213.

135 Ebd., S. 213.

136 Siehe ebd., S. 213.

137 Ebd., S. 213.

138 Siehe David Chaum. „Security without Identification: Transaction Systems to Make Big Brother Obsolete". In: *Communications of the ACM* 28.10 (1985), S. 1030–1044.

139 Einführend siehe auch Jarvis, *Crypto Wars*, S. 36–37. Jarvis fasst dies wie folgt zusammen: „The appeal of cryptographic currencies to the cypherpunks was their decentralization. In combination with encryption and the anonymity infrastructure the cypherpunks were building, transactions could occur between two parties without the government's knowledge. If the government could not see transactions, they could not levy taxes, nor build a dossier society. Therefore, the cypherpunks

Bis aber auch die gewöhnliche Bevölkerung von kryptographisch implementierten *Währungen*, sogenannten *Kryptowährungen*, erfuhr, sollten noch einige Jahre vergehen.[140] Im Jahr 2008 wurde dann aber ein Artikel veröffentlicht, der die Ziele der Cypherpunks nach Dezentralität scheinbar auch in der Realität des Finanzwesens erreichen könnte. Der Titel des Artikels: *Bitcoin – A Peer-to-Peer Electronic Cash System*.[141] Verfasst von einer Person oder Personengruppe mit dem Pseudonym Satoshi Nakamoto, entwickelt der Text die Grundlage für die Verwendung einer dezentralen Blockchain-Technologie für ein digitales Zahlungssystem.[142]

Vielleicht mag es im Kontext der Cypherpunks umso überraschender sein, dass die Kryptowährung Bitcoin selbst keineswegs anonym, sondern lediglich pseudonym ist.[143] Denn jeder kann öffentlich einsehen, welche Adresse an welche Adresse wie viel Bitcoin gesendet hat. Damit wird Bitcoin ein durch und durch transparentes System, das durch die Blockchain-Technologie auch rückblickend eine Einsicht in alle Transaktionen ermöglicht. Warum aber galt Bitcoin lange Zeit trotzdem als *irgendwie* anonym?

Transaktionen können dann anonym sein, wenn es keine Verbindung der pseudonymen Bitcoin-Adresse zur persönlichen Identität gibt. Des-

---

believed cryptocurrencies had the potential to clog the very arteries surging power through the body politic, the government's beating heart would fall silent, and the era of crypto-anarchy could begin"; Jarvis, *Crypto Wars*, S. 37.

140 Der Begriff *Währung* kann ebenso intensiv und hitzig diskutiert werden wie Bitcoin selbst. Wenn es ein notwendiges Kriterium für den Begriff der Währung ist, dass es sich um eine durch eine Zentralbank herausgegebene Art von Geld handelt, dann erfüllen das Bitcoin und andere *Kryptowährungen* nicht. Trotzdem trifft der Begriff der Währung auch in dezentralen Systemen das, was Bitcoin sein möchte, am besten.

141 Siehe Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. URL: https://bitcoin.org/bitcoin.pdf (besucht am 15.04.2024).

142 Siehe einführend Anderson, *Security Engineering*, S. 685–695.

143 Siehe Hanna Halaburda, Miklos Sarvary und Guillaume Haeringer. *Beyond Bitcoin: Economics of Digital Currencies and Blockchain Technologies*. 2. Aufl. Cham: Palgrave Macmillan, 2022, S. 116; sowie Henri Arslanian. *The Book of Crypto: The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets*. Cham: Palgrave Macmillan, 2022, S. 138–139; ausführlicher und für einen Überblick über die Forschung siehe Niluka Amarasinghe, Xavier Boyen und Matthew McKague. „A Survey of Anonymity of Cryptocurrencies". In: *Proceedings of the Australasian Computer Science Week Multiconference. Sydney, Australia*. ACSW '19. Association for Computing Machinery, 2019, Artikel 2, insbesondere S. 4; einführend auch Anderson, *Security Engineering*, S. 693.

wegen *schien* es wohl lange Zeit so, als wäre Bitcoin in gewisser Weise anonym. In der Realität allerdings ist diese Verbindung oft in irgendeiner Weise gegeben.[144] Für staatliche Institutionen mit enormen Ressourcen – etwa für das FBI – ist eine Identifizierung dann jedenfalls realisierbar.[145] Zudem wurden mit der Popularität von Bitcoin und der im Laufe der Jahre doch erfolgenden Regulierung vieler Kryptobörsen sogenannte *Know Your Customer* (KYC) Policies eingeführt.[146] Zum Kauf von Bitcoin mit Dollar, Euro oder sonstiger Zentralbankwährung kann dann etwa eine Legitimation und Identifizierung mit Ausweisdaten erforderlich sein. Mit dieser Verbindung der Identität zur pseudonymen Adresse ist Anonymität weiter erschwert. Nun kennen jene Kryptobörsen und all jene Parteien, die auf deren Daten zugreifen können, die Transaktionen, die von einer bestimmten Bitcoin-Adresse mit jener Identität ein- und ausgehen.[147]

Verschiedene technologische Möglichkeiten wurden daher entwickelt, die zumindest einen gewissen Grad an Anonymität erreichen sollen, zum Beispiel durch eine Art des *Mixens* von Bitcoins.[148] Trotzdem ist Bitcoin weiterhin *by design* keine anonyme Kryptowährung. Hinzu kommt, dass Bitcoin in der Realität weniger dezentral ist als erhofft. Eine gewisse Zentralisierung ist nämlich möglich, indem einige wenige Parteien über einen großen Pool an Grafikprozessoren (GPU) zum Mining von Bitcoin verfügen.[149] Erfolgreichere Anonymität und Dezentralität erreichen dagegen sogenannte *Privacy Coins* wie zum Beispiel *Monero*.[150]

Das Besondere bei Bitcoin ist jedoch, dass dieses Beispiel auch heute noch zeigt, was das Ideal *Cypherpunks write code* bewirken soll: Für den gesellschaftlichen Erfolg brauchte es keine Gesetzgebungsverfahren, kei-

144 Siehe Amarasinghe, Boyen und McKague, „A Survey of Anonymity of Cryptocurrencies", S. 4.

145 Siehe Halaburda, Sarvary und Haeringer, *Beyond Bitcoin*, S. 116.

146 Siehe Arslanian, *The Book of Crypto*, S. 325, weiterführend S. 325–333.

147 Normativ betrachtet wäre dann zu fragen, wie KYC-Prozesse zu bewerten sind. Arslanian beispielsweise behauptet: „The good news is that some level of KYC has now became standard practice across fiat-to-crypto exchanges, especially for those that are looking to build a long-term institutional grade business"; ebd., S. 327. Die Cypherpunks dürften einer solchen normativen Einschätzung wohl nicht zustimmen.

148 Siehe zum Mixing Halaburda, Sarvary und Haeringer, *Beyond Bitcoin*, S. 117, sowie Arslanian, *The Book of Crypto*, S. 323.

149 Siehe zur Zentralisierung der Miningpools Halaburda, Sarvary und Haeringer, *Beyond Bitcoin*, S. 95–96, zur sogenannten *51 %-Attacke* S. 96–98.

150 Einführend dazu siehe ebd., S. 116–119.

nen Lobbyismus, kein Venture Capital.[151] Einzelne Personen oder eine kleine Gruppe waren in der Lage, ihre Fähigkeiten zum Entwickeln von Code einzusetzen, um schließlich die eigenen politischen Vorstellungen umzusetzen. Kryptographie ist damit nicht mehr nur irgendein Mittel zur vertraulichen Kommunikation. Teil I der Arbeit hat bereits auf theoretischer Basis verdeutlicht, dass mithilfe von Moderner Kryptographie Schutzziele wie Integrität und Authentizität erreicht werden können. Nun ist Kryptographie aber auch *in der Praxis* mehr als nur bloße interpersonelle Kommunikation zum vertraulichen Austausch von Inhalten.[152]

Wie das Beispiel der Kryptowährungen zeigt, geht es den Cypherpunks also nicht ausschließlich um vertrauliche Kommunikation. Nach Craig Jarvis lassen sich vier Ziele der Cypherpunks systematisieren: (1) ein ungehinderter Zugang zur Verschlüsselung; (2) anonyme Kommunikation; (3) Freiheit zu anonymen Finanztransaktionen; (4) die Entwicklung von Whistleblowing-Plattformen.[153] In Teil III der Arbeit werden wir uns aus normativer Perspektive mit (1), (2) und (4) auseinandersetzen. Aufgrund der gebotenen Fokussierung sollen hingegen Kryptowährungen und anonyme Finanztransaktionen in der vorliegenden Arbeit nicht über die bisherige Diskussion hinaus untersucht werden. Es bleibt die Aufgabe späterer Arbeiten, eine Ethik der Kryptographie auch auf Kryptowährungen anzuwenden.

Solche radikalen Ideen einer freien und zugänglichen Kryptographie, wie sie auf den vorangehenden Seiten skizziert wurden, blieben auch in der Zivilgesellschaft und der Politik nicht lange unbemerkt. Ein Jahr nach Gründung der Cypherpunks erschien in der Zeitschrift *Wired* ein Artikel mit dem Titel *Crypto Rebels*.[154] Darin diskutiert der Cypherpunk-Kenner Steven Levy das ehemalige Monopol der NSA, und Zimmermanns PGP sowie die Cypherpunks werden einer breiteren Öffentlichkeit vorgestellt. Wenig überraschend waren aber nicht alle Reaktionen auf diese neue Art des Aktivismus positiver Natur.[155] Eine grundsätzliche Ablehnung von

151 Nach dem Erfolg von Bitcoin änderte sich dies natürlich im Laufe der Jahre. Entscheidend ist hier aber der Anfang der Entwicklung von Bitcoin.

152 Auf technischer Ebene ist Kryptographie selbstverständlich auch bei Kryptowährungen nicht mehr als ein Austausch von Information. Praktisch betrachtet ermöglicht sie hier aber völlig neue Anwendungsfälle.

153 Siehe zu diesen Zielen Jarvis, *Crypto Wars*, S. 34–38.

154 Siehe Steven Levy. „Crypto Rebels". In: *Wired* (1. Feb. 1993). URL: https://www.wired.com/1993/02/crypto-rebels/ (besucht am 15.04.2024).

155 Einführend siehe etwa im Kontext von PGP Jarvis, *Crypto Wars*, S. 224–228.

Regierungsgewalt und zentralisierter Macht, die sich nach Meinung der Cypherpunks in Überwachung, Zensur und Kontrolle manifestiert, erzwingt ja geradezu eine staatliche Antwort.

Diese Antipathie der Cypherpunks gegenüber staatlicher Gewalt und umgekehrt hat letztlich zu den sogenannten *Crypto Wars*[156] beigetragen, bei denen teils heftig über die Regulierung von Kryptographie, die Freiheit der Kommunikation und die Privatsphäre von Individuen gestritten wurde.[157] Dieser *Krieg* wurde zwar nicht mit Waffen geführt, sehr wohl aber mit Argumenten und Worten, zuweilen auch mit Polemik, Provokation und Übertreibung. Craig Jarvis fasst die Crypto Wars wie folgt zusammen:

> The crypto wars are framed using militaristic language, setting the belligerents to battle in an implied zero-sum game. The metaphorical invocation of warfare underlines the hostility existing between the parties. It also reflects the media-savy nature of the cypherpunks in sensationalizing their arguments in order to appeal to the media and amplify their message. The narrative is typically of security and privacy being in opposition, with the state benefiting from security (surveillance capabilities), and citizens from privacy (encryption).[158]

Im Rahmen von Teil III wird zu analysieren sein, inwieweit eine solche Dichotomie von Sicherheit und Privacy überhaupt notwendig ist. Was aber unabhängig davon bei vielen Narrativen der frühen Cypherpunks hervorsticht, ist eine Art Determinismus, eine Art natürliche Zwangsläufigkeit der Entwicklung. Die Gesetze der Mathematik seien schließlich die erfolgreicheren, die besseren Gesetze im Vergleich zu jenen der Regierungen und Staaten. Und da Kryptographie nun weitverbreitet war, *musste* die Crypto-Anarchie doch irgendwann Realität werden: „The universe believes in encryption"[159]. Diese fast schon quasi-religiöse Vorstellung über Kryptographie kann zu der Ansicht verleiten, dass eine Regulierung von Kryptographie kaum oder nur sehr schwer möglich sei – oder wie es Eric Hughes formuliert: „Even laws against cryptography reach only so far as

156 Als feststehender Begriff wird im Folgenden der englische Ausdruck genutzt. Einführend in die Crypto Wars siehe Anderson, *Security Engineering*, S. 925–934.

157 Der erste Crypto War begann nach Craig Jarvis bereits 1966; siehe Jarvis, *Crypto Wars*, S. 5.

158 Ebd., S. 5.

159 Assange u. a., *Cypherpunks*, S. 4.

a nation's border and the arm of its violence."[160] Doch ist die Macht und Gewalt des Staates wirklich so begrenzt? Wie das folgende Kapitel zeigen wird, ist eine systematische Regulierung von Kryptographie, die zumindest die *meisten* Menschen betrifft, durchaus möglich.

160 Hughes, *A Cypherpunk's Manifesto*.

4 Internet, Kryptographie und Regulierung

> Uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity.
>
> – Louis Freeh, damaliger Direktor des FBI[1]

Ist Kryptographie oder deren Anwendung regulierbar? Im letzten Kapitel ist deutlich geworden, dass manche Cypherpunks und die Crypto-Anarchie eine Art deterministische Vorstellung von Kryptographie verfolgen. Kryptographie *ist* nicht so einfach steuerbar, so einfach regulierbar.[2] Dieses *ist* meint dabei einen ontologischen Status, der den Gesetzen der Mathematik unterworfen sei – im Gegensatz zu menschengemachten Gesetzen oder staatlicher Gewalt.[3] Die Kryptographie als Teilbereich der Mathematik sei ein *anderes* Gesetz.[4] Wie Eric Hughes in *A Cypherpunk's Manifesto* schreibt:

> We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.[5]

Doch entspricht diese Vorstellung der Realität? Ist Kryptographie und deren Anwendung wirklich so unregulierbar, so unaufhaltsam? Die Beantwortung dieser Fragen erfordert einen systematischen Ansatz. Dabei

1 Louis J. Freeh. *Statement of Louis J. Freeh, Director Federal Bureau of Investigation. Before the Senate Judiciary Committee*. United States Senate. Washington D.C., 9. Juli 1997. URL: https://archive.epic.org/crypto/legislation/freeh_797.html (besucht am 15.04.2024); unter anderem zitiert auch in Jordan, *Information Politics*, S. 104.

2 Siehe etwa May, *The Crypto Anarchist Manifesto*, sowie May, *The Cyphernomicon*. May schreibt in seinem *Cyphernomicon* über die Crypto-Anarchie: „External force, law, and regulation cannot be applied. This is 'anarchy,' in the sense of no outside rulers and laws"; ebd.

3 Jacob Appelbaum, Mitentwickler von *Tor*, sagt auch: „One must acknowledge with cryptography no amount of violence will ever solve a math problem." In Assange u. a., *Cypherpunks*, S. 61.

4 Deutlich wird dies auch an Gilmores Vorstellung: „I want to guarantee – with physics and mathematics, not with laws – things like real privacy of personal communication". Zitiert in Levy, *Crypto*, S. 208.

5 Hughes, *A Cypherpunk's Manifesto*.

gehen wir in Abschnitt 4.1 zunächst von der Beobachtung aus, dass die Nutzung von Kryptographie und das Internet eng zusammenhängen. Das Internet wäre ohne Public-Key-Kryptographie, ohne digitale Signaturen, ohne eine integre Kommunikation nicht zu dem geworden, wie wir es heute kennen. Umgekehrt wäre es ohne die Infrastruktur des Internets niemals möglich gewesen, die Kryptographie in globaler Dimension zu verbreiten. In diesem Kontext wird Abschnitt 4.1 zeigen, dass auch für das Internet die verbreitete Vorstellung dominierte, ein nicht zu regulierender Raum zu sein.

Diese Auseinandersetzung wird zur methodischen Frage führen, ob Erkenntnisse aus dem Bereich der Internet Policy auch auf die Kryptographie (insbesondere *im* Internet) angewendet werden können. Abschnitt 4.2 wird sich dabei auf die einflussreichen Werke *Code: Version 2.0* von Lawrence Lessig sowie *Who Controls the Internet?* von Jack Goldsmith und Tim Wu stützen. Beide Arbeiten konnten in den 2000er-Jahren überzeugend darlegen, dass das Internet eben kein unregulierbarer Ort ist. Damals wie heute funktioniert eine solche Regulierung allerdings nicht *direkt*, sondern über *Intermediäre* wie etwa Internetanbieter.

Mit diesem Vorwissen wird in Abschnitt 4.3 schließlich eine systematische Einordnung von Regulierbarkeit und Steuerung von Kryptographie möglich. Dabei können wir auf umfassende historische Beispiele aus dem Kontext der bereits genannten Crypto Wars zurückgreifen. Neuere Methodiken, die durch maschinelles Lernen möglich geworden sind, werden ebenso diskutiert (insbesondere das sogenannte *Client-Side-Scanning*).[6] Das folgende Kapitel wird zusammenfassend zu dem Schluss kommen, dass Regulierung und Beschränkung der Nutzung von Kryptographie theoretisch und praktisch möglich ist – mit allen gesellschaftlichen und ethischen Implikationen.

4.1 Internet und Kryptographie

Zunächst handelt es sich bei der Kryptographie und dem Internet um zwei grundverschiedene Konzepte. Das Internet ist ein technologiebasiertes Netzwerk zur Kommunikation. Kryptographie hingegen ist, wie Teil I der Arbeit aufgezeigt hat, im Sinne Moderner Kryptographie ein

6 Zum Client-Side-Scanning siehe aus ethischer Diskussion insbesondere Abschnitt 8.1.

Teilbereich der Mathematik, der in Technologien Anwendung findet. Dies bedeutet, dass Kryptographie und kryptographische Protokolle auch ohne das Internet existieren können. Zum Beispiel kann Kryptographie im klassischen Briefverkehr Anwendung finden. Ein Protokoll wie der DH-Schlüsselaustausch ließe sich ohne Probleme in Schriftform durchführen, lediglich ein Taschenrechner mit einer gewissen Rechenkapazität wäre für beide kommunizierenden Parteien vonnöten. Zur Zertifizierung der Schlüssel könnte entweder eine Zertifizierung ähnlich wie bei PGP erfolgen, oder die Parteien bestätigen die Zertifikate über einen weiteren Kanal (z. B. per Telefon).[7]

Andererseits ist das Internet aber auch *mehr* als bloße Kryptographie. Auf der Applikationsebene des Internets bilden sich die unterschiedlichsten Geschäftsmodelle, soziale Netzwerke, Handelsbörsen, Online-Spiele und vieles mehr. In den 1990er- und 2000er-Jahren sprach man daher auch vom heute etwas archaisch klingenden *Cyberspace*. Für Lessig ist der Cyberspace eben mehr als das Internet: „though built on top of the internet, cyberspace is a richer experience“[8]. Er erkennt zwar, dass es keine scharfe Trennung von Internet und Cyberspace geben mag.[9] Das entscheidende Kriterium, das allerdings doch eine Differenz ermöglicht, ist für ihn das folgende:

> Cyberspace, by contrast, is not just about making life easier. It is about making life different, or perhaps better. It is about making a different (or second) life. It evokes, or calls to life, ways of interacting that were not possible before.[10]

Als Beispiel dient ihm hier das Computerspiel *Second Life*, das zur damaligen Zeit breite Aufmerksamkeit fand, aber auch *American Online* oder *Counsel Connect*.[11] Die Analogie heute wäre im engeren Sinne wohl Social Media. Mit etwas mehr sensueller Erfahrung sind auch *Virtual Reality* (VR) oder *Augmented Reality* (AR) zu nennen. Für die folgenden Argumente spielt die Unterscheidung von Cyberspace und Internet allerdings eine untergeordnete Rolle. Indem die Grundlagen *des* Internets und die Erfahrungswelt *im* Internet immer weiter verschwimmen, wird auch die

7 Siehe dazu die Ausführungen zu PGP in Abschnitt 3.1.
8 Lessig, *Code*, S. 9.
9 Siehe ebd., S. 9.
10 Ebd., S. 83.
11 Siehe ebd., S. 88-97.

Trennung der nihilistischen Technologie und der subjektiven Erfahrung zweitrangig.

Die Kryptographie ist also zunächst vom Internet respektive Cyberspace konzeptuell zu unterscheiden. Andererseits steht sie aber in einem engen Verhältnis zum Internet, insofern sie für dessen Nutzbarkeit eine *notwendige Bedingung* ist. Ohne kryptographische Protokolle wären Banktransaktionen nicht integer, Gesundheitsdaten nicht verschlüsselbar, private Kommunikation weder vertraulich noch sicher. Im letzten Kapitel ist die Verschlüsselungssoftware *Pretty Good Privacy* als ein Beispiel für Cryptoaktivismus vorgestellt worden.[12] PGP war ja gerade notwendig wegen des *eigentlich* unsicheren, nicht vertraulichen Internets.[13]

Grundlage dieses Verhältnisses war und ist die fundamentale Architektur des Internets als ursprüngliches Peer-to-Peer-Netzwerk, das auf einem zentralen Prinzip basiert: dem *Ende-zu-Ende-Prinzip*, kurz *E2E-Prinzip* (engl. *End-to-End Principle*).[14] Saltzer, Reed und Clark beschrieben dieses Designprinzip in ihrem 1981 erschienenen Artikel *End-to-End Arguments in System Design*.[15] Sie nennen dabei explizit Sicherheit durch Verschlüsselung als ein Anwendungsbeispiel des Prinzips, wobei sie drei Argumente anführen, warum die Verschlüsselung nicht von der Datenübertragung selbst durchgeführt werden sollte, sondern von der Applikation:

12 Ohne das Internet wären auch kryptographische Protokolle und deren Anwendung nicht so ubiquitär, wie sie es heute sind. Der von Zimmermann entwickelte Code hätte niemals die globale Dimension und die politische Bedeutung erlangt, wäre da nicht die Verbreitung über das Internet möglich gewesen. Siehe zum Verhältnis von Internet und PGP Levy, *Crypto*, S. 196–198.

13 Auch Rivest, Shamir und Adleman nennen in ihrem Artikel explizit E-Mails. Siehe Rivest, Shamir und Adleman, „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", S. 120.

14 Siehe zur Argumentation von Lessig und zum E2E-Prinzip Lessig, *Code*, S. 44–45 sowie S. 111–112. Alternativ kann vieles innerhalb der Diskussion um Internet Policy auch auf den inhärenten Aspekt der *Openess* zurückgeführt werden, wie ihn Jordan beschreibt. Siehe Jordan, *Information Politics*, S. 105–106.

15 Siehe Jerry H. Saltzer, David P. Reed und David D. Clark. „End-to-End Arguments in System Design". In: *Proceedings of the Second International Conference on Distributed Computing Systems*. 1981, S. 509–512; in der revidierten und umfassenderen Version auch Jerry H. Saltzer, David P. Reed und David D. Clark. „End-to-End Arguments in System Design". In: *ACM Transactions in Computer Systems* 2.4 (1984), S. 277–288. Im Folgenden bezieht sich die Diskussion auf den Artikel von 1984. Siehe weiterführend auch Tarleton Gillespie. „Engineering a principle: 'End-to-End' in the design of the internet". In: *Social Studies of Science* 36.3 (2006), S. 427–457.

> First, if the data transmission system performs encryption and decryption, it must be trusted to manage securely the required encryption keys. Second, the data will be in the clear and thus vulnerable as they pass into the target node and are fanned out to the target application. Third, the *authenticity* of the message must still be checked by the application. If the application performs end-to-end encryption, it obtains its required authentication check, it can handle key management to its satisfaction, and the data is never exposed outside the application.[16]

Komplexität wird mit dem E2E-Prinzip an den Rand des Netzwerks geschoben.[17] Damit wird die implementierte Kryptographie aber zur notwendigen Bedingung einer sicheren und vertraulichen Kommunikation im Internet. Ohne Kryptographie auf Anwendungsebene wäre das Internet ein Ort ohne Informationssicherheit. Auf ähnliche Weise wird diese Notwendigkeit deutlich bei Tim Jordan, der im Kontext der *Offenheit* des frühen Internets zu Recht erkennt:

> The internet was designed as an open platform almost accidentally, with early infrastructures far more concerned about connecting nodes of its network than securing identities or communication.[18]

Soweit zum technologischen Hintergrund des Verhältnisses von Kryptographie und Internet. Phänomenologisch zeigt sich aber auch, dass die Vorstellungen und Ideen *über* das Internet und den Cyberspace überraschend ähnlich sind zu denen *über* die Kryptographie. Für beides gilt nämlich, dass die Technologie mehr ist als nur eine reine Binärdarstellung von Nullen und Einsen. Hinter beiden Konzepten steht eine soziale, gesellschaftliche und anthropozentrische Lebenswirklichkeit, die erst realisierbar wurde durch die neuen, technologischen Möglichkeiten. Genauso wie die Moderne Kryptographie verleitete das Internet zur radikalen Utopie einer neuen Gesellschaft. In den Worten von Julian Assange war es „our greatest tool of emancipation"[19]. Nach Edward Snowden war dieses frühe Internet geprägt durch einen „cooperative, collectivist free-culture ethos"[20]. Und für den einflussreichen Kryptographen Ross Anderson wa-

16 Saltzer, Reed und Clark, „End-to-End Arguments in System Design", S. 282–283, kursiv im Original.
17 Siehe Lessig, *Code*, S. 44.
18 Jordan, *Information Politics*, S. 105.
19 Assange u. a., *Cypherpunks*, S. 1.
20 Snowden, *Permanent Record*, S. 46.

ren viele der Pioniere des Internets Utopistinnen und Utopisten: „we believed that free access to information would be liberating at the personal level, and would destabilise authoritarian governments too."[21]

Es fällt auf, dass sich viele der Motive und Ziele der Crypto-Anarchie mit den Vorstellungen über das frühe Internets decken. Man dachte, das Internet sei *natürlicherweise* frei und *natürlicherweise* nicht zu regulieren.[22] Nicht einmal durch eine normgebende Entscheidung der Regierungen der industriellen Welt, die im Cyberspace ohnehin nicht willkommen seien.[23] Kein Einfluss von außen sollte und konnte das Internet beeinflussen. Das Internet sollte ein selbstregulierender Raum sein – oder wie es David Clark, späterer Professor am MIT, einmal formulierte: „We reject: kings, presidents, and voting. We believe in: rough consensus and running code."[24] Lessig fasst solche Ansichten in pointierter Weise zusammen:

> If there was a meme that ruled talk about cyberspace, it was that cyberspace was a place that could not be regulated. That it "cannot be governed"; that its "nature" is to resist regulation. Not that cyberspace cannot be broken, or that government cannot shut it down. Buf if cyberspace exists, so first-generation thinking goes, government's power over behavior there is quite limited. In its essence, cyberspace is a space of no control.[25]

Eine grundlegende Haltung zu dieser Unregulierbarkeit kann begleitet werden durch Motive wie Anonymität, Dezentralisierung und Freiheit.

---

21 Anderson, *Security Engineering*, S. 909–910.

22 Siehe Lessig, *Code*, S. 3. Lessig spricht zwar vom Cyberspace, allerdings gilt dies auch für das Internet an sich, wenn der oben vorgenommenen Begriffsdiskussion gefolgt wird.

23 Siehe Barlow, *A Declaration of the Independence of Cyberspace*; dazu auch Abschnitt 3.2.

24 Zitiert z. B. in Andrew L. Russell. „'Rough Consensus and Running Code' and the Internet-OSI Standards War". In: *IEEE Annals of the History of Computing* 28.3 (2006), S. 48–61, hier S. 48; sowie in Paulina Borsook. „How Anarchy Works: On location with the masters of the metaverse, the Internet Engineering Task Force". In: *Wired* (1. Okt. 1995). URL: https://www.wired.com/1995/10/ietf/ (besucht am 15.04.2024); ebenfalls zitiert in Lessig, *Code*, S. 2.

25 Ebd., S. 31 Er fügt allerdings an, dass seiner Meinung nach Skepsis geboten sei: „Nature. Essence. Innate. The way things are. This kind of rhetoric should raise suspicions in any context. It should especially raise suspicions here. If there is any place where nature has no rule, it is in cyberspace. If there is any place that is constructed, cyberspace is it. Yet the rhetoric of 'essence' hides this constructedness. It misleads our intuitions in dangerous ways"; ebd., S. 31.

Es spielte zunächst wohl keine allzu große Rolle, ob das Internet in dieser Form *wirklich* so anonym war, wie man dachte (oder erhoffte). Das Design des Internets *per se* ist nämlich weder anonym noch sicher, wie weiter oben diskutiert worden ist. Wer sicher kommunizieren wollte, konnte dies zwar technisch erreichen, etwa mit PGP. Wer das allerdings nicht tat, für den war das Internet nur ein scheinbarer Ort der Anonymität und Sicherheit. Konsequenterweise meint Crypto-Anarchie für May denn auch „a society in which individuals must protect their own secrets and not count on governments or corporations to do it for them“[26].

Damit zusammen hängt das System der Dezentralität, denn wenn Verantwortung durch das E2E-Prinzip an den Rand des Netzwerks verschoben wird, fördert und fordert dies Dezentralität. Diese Dezentralität kann nun zur Ansicht verleiten, das Internet sei *grenzenlos* und *unzensierbar*. Obschon Staaten und Nationen physische Grenzen kontrollieren könnten – das Internet würde diese überwinden: „On the Information Highway, borders are just speed bumps.“[27] Oder wie das bekannt gewordene Zitat von John Gilmore sagt: „The Net interprets censorship as damage and routes around it“[28].

Das Motiv der Freiheit hängt wiederum eng mit dem Gedanken einer solchen Unregulierbarkeit zusammen: Individuen, die einen Zugriff auf einen Computer und das Internet hatten, konnten in jenem *Cyberpace*, dem „new home of Mind“[29], Schöpferin und Schöpfer eigener Welten werden. Die Grundüberzeugung war dabei, dass dann, wenn jemand keinen Körper habe, wie es im Cyberspace der Fall sei, man auch nicht

26 Zitiert in Greenberg, *This Machine Kills Secrets*, S. 90–91. Tim Jordan erkennt daher im Kontext der *Offenheit* der Internetarchitektur zu Recht: „This openness combines with the nature of the internet's address space so that the default state of the internet has been total identification of the origin computer and the receiving computer (as well as hops in between) and openness of the contents of data packets“; Jordan, *Information Politics*, S. 106.

27 Levy, *Crypto*, S. 198.

28 Zitiert in Philip Elmer-Dewitt. „First Nation in Cyberspace“. In: *TIME International* (6. Dez. 1993). URL: https://web.archive.org/web/20210408023213/https://kirste.userpage.fu-berlin.de/outerspace/internet-article.html (besucht am 15.04.2024). Weiterführend zum Hintergrund auch Richard Rogers. „The Internet Treats Censorship as a Malfunction and Routes Around it? A New Media Approach to the Study of State Internet Censorship“. In: *Spam Book: On Viruses, Porn and Other Anomalies from the Dark Side of Digital Culture*. Hrsg. von Jussi Parikka und Toni D. Sampson. Cresskill: Hampton Press, 2009, S. 229–247.

29 Barlow, *A Declaration of the Independence of Cyberspace*.

physisch genötigt werden könne.[30] Wie John Perry Barlow in seiner *Unabhängigkeitserklärung des Cyberspace* auch schreibt:

> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.[31]

Aus heutiger Perspektive wirkt die Vorstellung solcher *anonymer, grenzenloser Freiheit* womöglich fremd. Unverschlüsselte Kommunikation im Internet war schließlich wenig anonym, Firewalls und Filter waren theoretisch denkbar. Und die geistige, schöpferische Freiheit war nicht ohne physische Repräsentation in Mensch und Technik möglich. Aber hätte man bereits in den 1990er-Jahren erkennen können, dass die Wahrheit komplexer ist? Dass das Internet nicht die erhoffte Anarchie zur Folge hatte? Und dass eine solche ontologische Natürlichkeit eben doch nicht gegeben ist? Die Ähnlichkeiten von einer Vorstellung über die Kryptographie und einer Vorstellung über die Natur des Internets scheinen unübersehbar, weshalb wir fragen sollten: Wie konnte das Internet dann doch regulierbar werden?

4.2 Warum das Internet doch regulierbar ist

Fast dreißig Jahre nach der Veröffentlichung der *Unabhängigkeitserklärung des Cyberspace* durch Barlow zeigt die Realität: Das Internet ist nicht der erhoffte rechtsfreie Wilde Westen geblieben. Nationen überall auf der Welt haben Gesetze verabschiedet, was Unternehmen und Personen im Internet dürfen, was sie nicht dürfen, welche Technologie zu fördern ist oder welche Dienste das Internet zu bieten hat. Auch die Vereinten Nationen haben bereits mehrfach betont, dass die Rechte, die die Menschen offline haben, auch online geschützt werden müssen.[32] Für die frühen

30 Barlow, *A Declaration of the Independence of Cyberspace*.

31 Ebd.

32 Siehe Human Rights Council. *The promotion, protection and enjoyment of human rights on the Internet*. A/HRC/RES/20/8. 2012, S. 2; auch Human Rights Council. *The right to privacy in the digital age*. A/HRC/RES/42/15. 2019, S. 4. Teil III der Arbeit wird sich kritischer mit einer solchen Forderung auseinandersetzen.

Verfechterinnen und Verfechter des freien Internets mag es vielleicht sogar erwartbar gewesen sein, dass Regierungen, Staaten und Konzerne über das Internet bestimmen *wollen*; viel überraschender musste aber sein, dass solche Bestimmungen tatsächlich auch funktionieren.[33] Immerhin war es ja der Kern dieser Internet-Philosophie, dass das Internet *natürlicherweise* frei war – egal, was die Mächtigen der Welt dazu dachten.[34] Was hatte sich geändert? Wodurch wurde das Internet zum regulierbaren und regulierten Raum?[35]

Zunächst ist eine basale Erkenntnis für die folgenden Ausführungen notwendig. Für Barlow war der Cyberspace zwar womöglich unregulierbar oder gar metaphysisch: „Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion."[36] Jedoch baut dieser *Raum* letztlich auf physikalisch-technischen Grundlagen auf, die durchaus kontrollierbar sind. Viele Jahre nach Barlows Unabhängigkeitserklärung erkennt selbst der Cypherpunk Julian Assange in pointierter Weise, dass Kontrolle über dieses „platonic realm"[37] möglich ist:

> The platonic nature of the internet, ideas and information flows, is debased by its physical origins. Its foundations are fiber optic cable lines stretching across the ocean floors, satellites spinning above our heads, computer servers housed in buildings in cities from New York to Nairobi. Like the soldier who slew Archimedes with a mere sword, so too could an armed militia take control of the peak development of Western civilization, our platonic realm.[38]

Tatsächlich aber ist die Situation einer Regulierung *im* Internet und *des* Internets noch weitaus komplexer. Um uns dieser Thematik systematisch annähern zu können, werden wir im Folgenden zwei einflussreiche Arbeiten diskutieren, die sich beide mit diesen Fragen auseinandersetzen: mit *Code: Version 2.0* von Lawrence Lessig und mit *Who Controls the Internet?* von Goldsmith und Wu. Beide Werke gaben in den 2000ern entscheidende Impulse zur Regulierung des Internets, die bis heute nichts an Anwendbarkeit und Aktualität eingebüßt haben. Dieser Abschnitt stellt

33 Siehe Lessig, *Code*, S. 3.
34 Siehe ebd., S. 3 sowie S. 31.
35 Man könnte hier auch vom Prozess einer *securitisation* sprechen. Siehe die Diskussion bei Jordan, *Information Politics*, S. 104–105.
36 Barlow, *A Declaration of the Independence of Cyberspace*.
37 Assange u. a., *Cypherpunks*, S. 3.
38 Ebd., S. 3.

daher zunächst die beiden zueinander komplementären Frameworks vor, sodass sie im nachfolgenden Abschnitt auf die Regulierung von Kryptographie angewandt werden können.

Beschäftigen wir uns zunächst mit Lessigs *Code*. In Kapitel 7 mit dem Titel *What Things Regulate* fragt Lessig, wie Individuen reguliert werden können. Den Ansatz, den er entwickelt, nennt er nach einem gleichnamigen Artikel von 1998 auch „The New Chicago School“[39]. Im Kontext von John Stuart Mills Freiheitskonzeption geht er zunächst von der Frage aus, was *heute* die größte Gefahr für die Freiheit sei.[40] Historisch hätten dies Normen, der Markt sowie staatliche Unterdrückung sein können. Allerdings sei mit dem Cyberspace ein neuer „regulator“[41] und ein „threat to liberty“[42] hinzugekommen: der *Code* – also das, was er beschreibt als „the instructions embedded in the software or hardware that makes cyberspace what it is“[43].

Lessig erkennt nun aber auch, dass Regulierung durch Code eben nicht dazu führt, dass Normen, staatliche Macht und der Markt obsolet werden würden.[44] Darin unterscheidet er sich von den Narrativen der Internet-Utopistinnen und -Utopisten, die dachten, *nur noch* Code würde die Zukunft bestimmen. Wie Lessig herausarbeitet, ist dieser Code nicht völlig von den „more traditional threats“[45] für die Freiheit losgelöst.[46] Er entwickelt darauf aufbauend einen umfassenden Ansatz, der die vier Bedingungen der Regulierung – Normen, Gesetze, Markt und Architektur – inkludiert, die er als *Modalitäten* oder *Constraints* bezeichnet.[47] Im Folgenden sollen diese Modalitäten anhand von Lessigs Ausführungen beschreiben werden, um sie anschließend in Abschnitt 4.3 auf die Kryptographie anwenden zu können.

39 Lawrence Lessig. „The New Chicago School“. In: *The Journal of Legal Studies* 27.S2 (1998), S. 661–691. Siehe auch Lessig, *Code*, S. 340, zur Erklärung des Ansatzes S. 340–345.

40 Siehe dazu und zum Folgenden ebd., S. 120–121.

41 Ebd., S. 121.

42 Ebd., S. 121.

43 Ebd., S. 121.

44 Siehe ebd., S. 121.

45 Ebd., S. 121.

46 Siehe ebd., S. 121.

47 Siehe dazu und zum Folgenden ebd., S. 123-124.

Lessig greift das Beispiel des Rauchens auf und fragt, welche Beschränkungen hier für das Individuum vorhanden seien.[48] Zunächst bestimme das *Gesetz*, wem es wo erlaubt sei, zu rauchen. Dies ist für Lessig aber nicht die signifikanteste Beschränkung. Hinzu komme nämlich, dass auch *Normen* das Rauchen oder Nichtrauchen beeinflussten. Normen würden etwa bestimmen, dass man sich im Auto keine Zigarette anstecke, ohne vorher Mitfahrende um Erlaubnis gebeten zu haben. Die dritte Modalität zeigt sich für Lessig darin, dass auch der *Markt* in Form des Preises oder der Qualität der Zigaretten einen Einfluss auf die Beschränkung des Rauchens nimmt. Und zuletzt die *Architektur*: Wie eine Zigarette aufgebaut ist, ob sie Nikotin enthält, wie sie entworfen ist – all das bestimme, wie Rauchen eingeschränkt werden könne.

Das andere Beispiel, das Lessig nennt, bezieht sich direkt auf den Cyberspace. Das *Gesetz* reguliere Verhalten im Cyberspace, zum Beispiel durch Urheberrechtsgesetze.[49] Gleiches gelte für *Normen*. Lessig denkt hier an Online-Communitys, in denen manches Verhalten erwünscht oder unerwünscht sei. Aber auch der *Markt* reguliere Verhalten, zum Beispiel durch Preisstrukturen, Abonnementmodelle oder Zugriffsbeschränkungen. Und zuletzt die Architektur, die Lessig im Cypberspace als *Code* definiert: wie eine Applikation aufgebaut ist, welche Möglichkeiten sie bietet, was sie verhindert.[50] All das bedeutet für Lessig: „Code embeds certain values"[51]. An anderer Stelle führt er dazu weiter aus:

> As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed. They are the ones who set its nature.[52]

Lessig spricht auch von seinem prägnanten und viel zitierten „code is law"[53]. Unübersehbar ist hier die Parallele zu Eric Hughes' „Cypherpunks write code"[54]. Nicht Normen, nicht der Markt, nicht das Gesetz – sondern

48 Siehe dazu und zu diesem Absatz ebd., S. 122–123.
49 Siehe dazu und zu diesem Absatz ebd., S. 124–125.
50 Als explizites Beispiel nennt er hierbei auch die verschlüsselte Kommunikation; siehe ebd., S. 125.
51 Ebd., S. 125, weiterführend auch S. 77.
52 Ebd., S. 79.
53 Ebd., S. 5. Siehe dazu und zu Lessig auch Webb, *Coding Democracy*, S. 53–56.
54 Hughes, *A Cypherpunk's Manifesto*.

Code ist Mittel und Regulierer im digitalen Zeitalter.[55] Oder um es mit den Worten von Julian Assange zu beschreiben: „One of the fundamental things the cypherpunks recognized is that the architecture actually defines the political situation."[56]

Doch im Gegensatz dazu erkennt Lessig auch, dass sich Modalitäten gegenseitig beeinflussen.[57] Für Regierungen und Staaten bedeutet das, dass sie mit Gesetzen die anderen Modalitäten beeinflussen können: Per Gesetz könne der Markt gesteuert werden, etwa mit Besteuerung oder Subventionierung; Gesetze beeinflussen aber auch soziale Normen, etwa durch Bildung; und Gesetze steuern die Regulierung von Architekturen, etwa mit Fahrbahnschwellen in Parkhäusern zur Geschwindigkeitsreduktion.[58] Lessig stellt fest, dass das Recht somit zwischen *direkter* und *indirekter* Regulierung unterscheidet:

> When its operation is direct, it tells individuals how to behave and threatens punishment if they deviate from that behavior. When its operation is indirect, it modifies one of the other structures of constraints.[59]

Damit wird der systematische Unterschied beschrieben von einem Gesetz, das etwa *direkt* das Rauchen für bestimmte Altersgruppen verbietet, und einem Gesetz, das per Steuererhöhung den Preis von Zigaretten anhebt und so *indirekt* den Konsum einschränkt. Bei der Entscheidung, wie der Gesetzgeber und das Recht vorgehen sollen, handelt es sich um einen Trade-off unterschiedlicher Modalitäten: Welche Modalität kann das Ziel (etwa Reduktion von Zigarettenkonsum oder Diskriminierung) zu den geringsten Kosten erreichen?[60] Bezogen auf die Kryptographie handelt

55 Die Ähnlichkeit von *Code is Law* zu den Vorstellungen der Cypherpunks ist auch daran ersichtlich, dass Julian Assange diesen Gedanken fälschlicherweise den Cypherpunks zusprach; siehe Assange u. a., *Cypherpunks*, S. 153. Auch Craig Jarvis verweist auf diese Beziehung von *Code is Law* zum cypherpunkishen *Writing Code*; siehe Jarvis, *Crypto Wars*, S. 38–39, sowie Berret, „The Cultural Contradictions of Cryptography", S. 6.

56 Assange u. a., *Cypherpunks*, S. 90.

57 Siehe Lessig, *Code*, S. 124.

58 Siehe ebd., S. 127–129.

59 Ebd., S. 132. Mit *constraints* sind die obigen Modalitäten gemeint. Lessig greift hier auch auf Polk Wagners Artikel *On Software Regulation* zurück; siehe dazu R. Polk Wagner. „On Software Regulation". In: *Southern California Law Review* 78.2 (2005), S. 457–520.

60 Siehe Lessig, *Code*, S. 130, zu Beispielen auch S. 130–132.

es sich in den meisten Fällen um eine solche *indirekte* Regulierung. Abschnitt 8.2 wird explizit normativ diskutieren, wie eine indirekte Beeinflussung im Vergleich zu einer direkten Regulierung einzuordnen ist.[61] Zur Präzisierung, warum Regulierung damit auch im Internet möglich ist, betrachten wir zunächst jedoch noch einen zweiten, komplementären Ansatz.

Zur Frage nach der Kontrollierbarkeit und Regulierbarkeit des Internets haben neben Larry Lessig insbesondere Jack Goldsmith und Tim Wu mit ihrem Werk *Who Controls the Internet? Illusions of a Borderless World* entscheidende Impulse liefern können. Goldsmith und Wu zeigen darin auf, wie sich das Internet zu Beginn des Jahrtausends gewandelt hat:

> It is the story of the death of the dream of self-governing cyber-communities that would escape geography forever. It is also the story of the birth and early years of a new kind of Internet – a bordered network where territorial law, government power, and international relations matter as much as technological invention.[62]

Ähnlich wie Lessig zeigen sie also auf, wie die Utopie des Cyberspace der Realität weichen musste, denn ihrer Meinung nach gilt: (1) Staatliche Gewalt und geographische Aspekte bleiben auch im Internet relevant.[63] (2) Das Internet wird geographisch stärker aufgeteilt und erhält eigene Grenzen (engl. *borders*). (3) Das so geographisch separierte Internet hat durchaus einige unerwartete Tugenden oder Vorteile (engl. *underappreciated virtues*).

Diesen Gedanken liegt zugrunde, dass es sich hierbei auch um eine Frage internationalen Rechts handelt. Zur Verdeutlichung mag folgendes Beispiel dienen: Gehen wir davon aus, dass im Staat X nationalsozialistische Propaganda verboten ist, im Staat Y aber nicht.[64] Im Staat Y wird jedoch ein Server betrieben, der solche Propaganda verbreitet. Was bedeutet dies für Staat X, wenn Personen auf dessen Hoheitsgebiet diese Propaganda über das Internet wahrnehmen können? Ist das Internet nun

61 Bereits Lessig hat sich damit teilweise normativ beschäftigt; siehe etwa ebd., S. 132–137.

62 Goldsmith und Wu, *Who Controls the Internet?*, S. xi.

63 Siehe dazu und zu den anderen zwei Aspekten ebd., S. xii. Die Ideen des Cyberspace zeigen sie ebenso an John Perry Barlows Vorstellungen. Siehe ebd., S. 17–22, allgemeiner auch S. 13–27.

64 Dieses Beispiel orientiert sich am Fall von Yahoo und Frankreich, den Goldsmith und Wu diskutieren; siehe ebd., S. 1–10.

wirklich so unregulierbar, dass keine Macht über den Server im anderen Staat ausgeübt werden kann? Bedeutet das, dass Propaganda nun auch in Staat X unausweichlich ist?

Zunächst könnte man hier annehmen, dass zuallererst Nationalstaaten für eine Abgrenzung im Internet sorgen wollten. Tatsächlich war dies jedoch, wie Goldsmith und Wu herausarbeiten, ein organisches Geschehen: Nutzerinnen und Nutzer auf der ganzen Welt haben unterschiedliche Bedürfnisse und Interessen.[65] Gerade heute und mit Blick auf individuelles Advertising und Target-Marketing scheint solch eine Abgrenzung aus marktwirtschaftlicher Perspektive unausweichlich gewesen zu sein. Das Internet fragmentiert sich selbst und wird, wie Goldsmith und Wu es nennen, „a connection of national and regional networks"[66].

Bei dieser Fragmentierung ist es ratsam, die einzelnen Schichten des Internets aus technologischer Perspektive etwas genauer zu unterscheiden.[67] Das bereits diskutierte E2E-Prinzip überträgt Autorität über Inhalt, Sicherheit und Darstellung auf die Ebene der Applikation, wodurch eine solche generische *Ab*-Grenzung ermöglicht wird. In diesem Sinn ist *Dezentralisierung* letztlich sowohl Ursprung als auch Folge eines abgegrenzten Internets. Die Applikationsebene und deren Inhalt sind zwar eher regional orientiert, die grundsätzliche Architektur des Internets ist davon jedoch nicht betroffen.[68]

Andererseits stellt sich unabhängig von diesen technologischen Aspekten die Frage, *wie* Regulierung im Internet und des Internets aus gesetzgeberischer Perspektive möglich sein kann. Auch hier legen Goldsmith und Wu überzeugend dar, dass territoriale Regierung und staatliche Gewalt nicht überflüssig werden.[69] Bezogen auf eine solche Regulierung greifen Goldsmith und Wu auf Lessig zurück und stellen zunächst fest: „The law need not to be *completely* effective to be *adequately* effective. All

65 Siehe Goldsmith und Wu, *Who Controls the Internet?*, S. 49.

66 Ebd., S. 57.

67 Auch Goldsmith und Wu erkennen dies, indem sie zusammenfassen: „This book has described three reasons why what we once called a global network is becoming a collection of nation-state networks – networks still linked by the Internet Protocol, but for many purposes separate"; ebd., S. 149.

68 Mit der Architektur ist die TCP/IP-Protokollarchitektur gemeint. Auch Lessig nimmt diese technologische Differenzierung vor und wendet seine Theorie explizit nicht auf eine Veränderung der TCP/IP-Architektur an. Siehe Lessig, *Code*, S. 143–145, vor allem S. 145.

69 Siehe Goldsmith und Wu, *Who Controls the Internet?*, S. 180–181.

the law aims to do is to raise the costs of the activity in order to limit that activity to acceptable levels."[70]

Goldsmith und Wu bauen in ihrer Systematik aber auch auf einen weiteren, entscheidenden Aspekt auf, der für die Regulierung von Kryptographie relevant ist: Gesetzliche Regulierung zielt häufig nicht *direkt* auf individuelles Verhalten ab, sondern auf *Intermediäre* – also Entitäten, die nicht das eigentliche Ziel der Regulierung sind, sondern die dazu genutzt werden, um das eigentliche Ziel zu erreichen.[71] Im scheinbar globalen Internet werden damit nicht ausländische Server oder im Ausland befindliche Personen Ziel der Regulierung, sondern lokale Entitäten wie etwa Internet Service Provider (ISP).[72] Es handelt sich somit für Goldsmith und Wu um eine extraterritoriale Kontrolle durch lokale Intermediäre.[73] Sie stellen dabei fest, dass Lessigs *Code is Law* und die Regulierung von Code eine Form der intermediären Kontrolle darstellen.[74] Intermediäre stehen also im Fokus dessen, was Lessig mit *indirekter* Regulierung beschreibt.

Diese *Intermediäre* sind von der *Quelle* und dem *Ziel* zu unterscheiden.[75] Manchmal liegen zwar alle drei Parteien auf dem Hoheitsgebiet ein und desselben Staates, wodurch dieser die Möglichkeit hat, jeden Einzelnen von ihnen zu sanktionieren. Die interessantere Frage allerdings

70 Ebd., S. 67, kursiv im Original. Goldsmith und Wu zitieren hier Lawrence Lessig. „The Zones of Cyberspace". In: *Stanford Law Review* 48.5 (1996), S. 1403–1411, hier S. 1405. Siehe etwa auch bei Lessig, *Code*, S. 59: „Not impossible, but difficult. Not for all people, but for enough to matter." Für eine ethische Analyse wird zu identifizieren sein, welche Effektivität „*adequately* effective" sein kann. Wie wäre etwa eine Regulierung von Kryptographie ethisch zu bewerten, wenn sie auch Personen betreffen würde, die überhaupt nicht das Ziel der infrage stehenden Regulierung sind? Wenn diese Personen letztlich vielleicht sogar am meisten davon betroffen wären, wäre eine adäquate Effektivität dann noch gegeben?

71 Siehe Goldsmith und Wu, *Who Controls the Internet?*, S. 68. Sie zitieren hier Levinson, der sich in seinem Artikel mit der Sanktionierung von Gruppen auseinandersetzt. Siehe Daryl J. Levinson. „Collective Sanctions". In: *Stanford Law Review* 56.2 (2003), S. 345–428.

72 Siehe Goldsmith und Wu, *Who Controls the Internet?*, S. 68–70. Internet Service Provider sind notwendige Dienstleister, die Unternehmen, Organisationen oder Personen mit dem Internet verbinden. Siehe einführend zu ISPs im Kontext der Überwachung auch Anderson, *Security Engineering*, S. 921–922.

73 Sie titulieren den Abschnitt entsprechend mit „Extraterritorial Control Through Local Intermediaries"; Goldsmith und Wu, *Who Controls the Internet?*, S. 68.

74 Siehe ebd., S. 72.

75 Siehe dazu und zu diesem Absatz ebd., S. 67–72.

ist: Was passiert, wenn *nur* die Intermediäre und Ziele im Hoheitsgebiet liegen, die Quelle aber außerhalb? Server, die aus dem Ausland heraus operieren, können auch aus anderen Staaten heraus aufgerufen werden. In dieser Situation ist zwar die Quelle nicht zu kontrollieren, die Intermediäre wie etwa Internet Service Provider allerdings schon. Entscheidend ist, dass solche Intermediäre selbst im Internet und im Bereich vertraulicher Kommunikation existieren.[76] In solchen Situation ist für staatliche Institutionen eine gesetzliche Regulierung und Kontrolle möglich und umsetzbar.

Verdeutlichen wir diese Kontrolle an einem Beispiel der Regulierung von Kryptographie. Gehen wir davon aus, dass ein Staat X die private Kommunikation von Messengerdiensten mitlesen möchte. Dazu wird er nicht direkt das Verhalten des Individuums regulieren, sondern kommerzielle und populäre Kommunikationsdienstleister verpflichten, dieses Abhören zu ermöglichen. Die Menschen, die die betreffenden Dienstleistungen nutzen, wären anschließend indirekt betroffen. Zwar würde das nicht bedeuten, dass es *überhaupt keine* Alternativen mehr gäbe. Beispielsweise könnten die Nutzerinnen und Nutzer zu freier Open-Source-Software wechseln, so etwa PGP.[77] Im Extremfall könnten Nutzende auch per Post kommunizieren und dabei die gleichen Algorithmen anwenden wie im Fall der Online-Kommunikation.

Eine solche Umgehung populärer Intermediäre sorgt allerdings für signifikante Einbußen an Komfort bis hin zur praktischen Unmöglichkeit.[78] Gerade bei Messengern ist es für deren praktische Anwendung von entscheidender Bedeutung, dass das Umfeld der Nutzenden den gleichen Kommunikationskanal oder die gleiche Applikation verwendet. Wenn sich eine Person dazu entscheidet, den Messenger zu wechseln, bedeutet dies, dass sie nicht mehr mit den Personen kommunizieren kann, die nicht gewechselt haben. Es handelt sich in diesem Beispiel also um eine einander bedingende Einbuße: Je geringer der Komfort, desto weniger werden

76 Die Alternative wäre, dass sowohl Quelle also auch Intermediäre im Ausland sind und sich nur das Ziel im Inland befindet. Tatsächlich ist eine solche Situation jedoch kaum realistisch. Wie Goldsmith und Wu argumentieren, wird es immer lokale Intermediäre geben. Siehe dazu Goldsmith und Wu, *Who Controls the Internet?*, S. 70–71.

77 Siehe Daniel Moore und Thomas Rid. „Cryptopolitik and the darknet". In: *Survival* 58.1 (2016), S. 7–38, hier S. 31.

78 Intermediäre machen nämlich viele Dinge einfacher; siehe Goldsmith und Wu, *Who Controls the Internet?*, S. 70.

alternative Messenger genutzt. Und je weniger Personen einen Messenger nutzen, desto weniger komfortabel ist er.

Zusammenfassend hat dieser Abschnitt damit analysieren können, dass entgegen der ursprünglichen Hoffnungen und Utopien auch eine Regulierung des Internets möglich ist. Wie das letzte Beispiel zur Regulierung von Kryptographie über Intermediäre zudem deutlich gemacht hat, sind das Internet und die *Anwendung* der Kryptographie nicht separierbar. Zwar sind die mathematischen Grundlagen der Kryptographie weitverbreitet, deren komfortable Anwendung hängt aber immer von den jeweiligen Kommunikationskanälen ab. Just jene Kanäle bieten nun auch im Bereich der Kryptographie die Möglichkeit einer gesetzlichen Regulierung durch Modalitäten und Intermediäre. Daher sollen im nächsten Kapitel die Erkenntnisse der letzten beiden Abschnitte im Fall der Kryptographie vertiefter diskutiert werden.

4.3 Und warum auch Kryptographie regulierbar ist

Das Ziel der *Einschränkung* von Kryptographie ist in fast allen Fällen die verschlüsselte Kommunikation, also das Schutzziel der Vertraulichkeit. Die Schutzziele der Integrität oder Authentizität sind hingegen von einer Einschränkung nicht betroffen, da hier kein Interessenkonflikt von Allgemeinwohl (z. B. Kriminalitätsbekämpfung) einerseits und den Rechten des Individuums (z. B. auf Privatsphäre) andererseits zu bestehen scheint.[79] Eine *Verpflichtung* zu kryptographischer Anwendung hingegen kann auch das Schutzziel der Authentizität inkludieren, etwa im Rahmen einer Ausweispflicht im Internet.[80] Dieses Kapitel wird sich mit beiden Fällen auseinandersetzen, wobei der Fokus auf der Einschränkbarkeit von vertraulicher Kommunikation liegen wird.[81]

79 Auch Diffie und Landau stellen fest, dass „the right to use cryptography for authentication is not in question; the right to use it for privacy is." Diffie und Landau, *Privacy on the Line*, S. 12.

80 Digitale Signaturen sind bereits Gegenstand von Policy-Diskussionen, auch wenn der Charakter und die Ziele dieser Policies grundlegend verschieden sind vom Schutzziel der Vertraulichkeit. Weiterführend dazu Hassan Aljifri und Diego Sánchez Navarro. „International legal aspects of cryptography". In: *Computers & Security* 22.3 (2003), S. 196–203.

81 Abschnitt 7.3 wird sich dann eingehender mit der ebenso wichtigen Frage nach Mechanismen der Identifizierung befassen.

Historisch betrachtet haben Regierungen, Strafverfolgungsbehörden und Geheimdienste die Nutzung von Kryptographie zur nachweisbar vertraulichen und sicheren Kommunikation lange Zeit kritisch betrachtet.[82] Kryptographinnen und Kryptographen haben dagegen immer wieder betont, dass eine ubiquitäre Kryptographie der allgemeinen Sicherheit dienlich ist, so etwa auch der nationalen Sicherheit.[83] Trotz dieser Gegenargumente gibt es bis heute Versuche, Kryptographie und deren Verwendung zu verbieten, zu schwächen oder zumindest zu erschweren. Die Möglichkeiten sind vielfältig und betreffen oftmals unterschiedliche Intermediäre und Modalitäten. Im Folgenden sollen sie aufgezeigt und systematisch eingeordnet werden.

Zunächst stellen wir uns dazu eine Situation vor, in der die Legislative eines Staates X entscheidet, dass verschlüsselte Kommunikation beschränkt und reguliert werden soll – nicht zwangsläufig für alle Personen, aber doch für die allermeisten. Es geht für sie daher nicht um eine absolute Verbannung, da sie wüsste, dass dies nur mit brachialen und unverhältnismäßigen Methoden möglich wäre. Sie möchte allerdings, dass die Kryptographie *ausreichend* reduziert wird. Außerdem möchte sie sich für mehr Identifizierung im Internet einsetzen. Die Gründe und die ethischen wie rechtlichen Probleme spielen an dieser Stelle keine Rolle, da es uns in diesem hypothetischen Fall lediglich um die *Möglichkeiten* der Regulierung gehen soll.

Zur Vereinfachung betrachten wir außerdem ausschließlich die interpersonelle Kommunikation, zum Beispiel über Messengerdienste. Dabei gehen wir von einer Situation aus, in der es in Staat X einige soziale Medien gibt, die ihre Messengerdienste mit einer Ende-zu-Ende-Verschlüsselung anbieten. Wir können auch davon ausgehen, dass ein, zwei oder höchstens drei dieser Dienstleister über enorme Marktanteile verfügen. Um die Möglichkeit der Regulierung von Kryptographie und ihrer Nutzung zu analysieren, sind in diesem Kontext zwei Fragen zu

82 Siehe z. B. die Diskussion um DES in Abschnitt 2.2.

83 Siehe etwa Susan Landau. „The National-Security Needs for Ubiquitous Encryption". In: *Don't Panic: Making Progress on the "Going Dark" Debate*. 1. Feb. 2016, Appendix A. URL: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (besucht am 15.04.2024). Landau argumentiert hierbei mit dem Schutz geistigen Eigentums: „Protecting U.S. intellectual property is crucial for U.S. economic and national security, and given BYOD [Bring Your Own Device] – a social change that is here to stay – encrypted communications are necessary for national security"; ebd., S. 2.

stellen: (1) Wie ließen sich Lessigs Modalitäten auf den Umgang mit Kryptographie anwenden? (2) Wie könnte eine indirekte Beschränkung der verschlüsselten Kommunikation (oder auch die Verpflichtung zur Identifikation über kryptographische Authentifizierung) über Intermediäre erfolgen?

Bezüglich der ersten Frage (1) wäre zunächst eine *direkte* Regulierung über die Modalität des *Rechts* möglich. Darunter würde das Verbot der Verwendung von kryptographischer und vertraulicher Kommunikation fallen. Wer etwa Algorithmen verwendet, die eine staatlich angeordnete Entschlüsselung verhindern können, müsste mit Strafen rechnen. Für die Gesetzgeber gäbe es dabei ein breites Spektrum möglicher Strafen, die von geringen Geldstrafen bis hin zu Gefängnisstrafen reichen könnten.[84] Es fallen aber auch durch den Gesetzgeber vorgegebene *Gebote* oder *Verpflichtungen* in die Modalität des Rechts. Im Kontext der Kryptographie könnte es sich beispielsweise um einen Zwang zur dauerhaften Authentifizierung im Internet handeln. Ein Verstoß der Bürgerinnen und Bürger gegen diese Aufforderung würde unter direkte Strafe gestellt werden.

Normen als zweite Modalität der Regulierung sind auf den ersten Blick weniger eindeutig. Aber auch hier lassen sich Verbindungen zur Kryptographie erkennen. So gilt es etwa als unverschämt und wird sozial geächtet, wenn eine unbefugte Person den Kommunikationskanal von zwei Parteien grundlos abhört und zu entschlüsseln sucht. Wird ein entsprechendes Verhalten publik, hat das daher zur Folge, dass die Person öffentlich kritisiert und ihr Verhalten geächtet wird. Vertrauliche Kommunikation ist somit durch soziale Normen geschützt. Gleichzeitig kann in gewissen Situationen eine Identifikation erwartet werden. In einer persönlichen Begegnung zweier Menschen werden beide Parteien davon ausgehen, dass die jeweils andere sich vorstellt. Zumindest in gewissem Maße kann dies auch online und im Internet erwünscht sein.

Der *Markt* als dritte Modalität kann ebenso im Kontext der Kryptographie betroffen sein. Als Beispiel sei hier genannt, dass Nutzende unterschiedliche Forderungen an den Markt stellen, etwa was den Preis des Produkts angeht. Sollten Produkte wie Messengerdienste, die eine Ende-zu-Ende-Verschlüsselung anbieten, signifikant teurer sein als solche ohne, dann könnte davon ausgegangen werden, dass ein großer Teil der Bevöl-

84 Ob eine solche Strafandrohung verhältnismäßig wäre, soll im Moment nicht weiter diskutiert werden.

kerung auf diese Verschlüsselungsprodukte verzichtet. Bei gleichem Preis und Komfort werden jedoch die wohl meisten Menschen einen Dienst mit Verschlüsselungstechnologie bevorzugen. Dies kann daher ein Anreiz für Unternehmen sein, die Entwicklung von verschlüsselter Kommunikation zu fördern. Die Veröffentlichung von Daten durch Hackerangriffe, die zu einer Identifikation der Nutzerinnen und Nutzer führt, würden sich hingegen schädigend auf das betreffende Unternehmen auswirken.

Die allergrößten Konsequenzen dürfte aber die *Architektur* respektive der *Code* als die vierte Modalität haben. Wenn Produkte keine Verschlüsselungstechnologie implementieren, dann ist eine vertrauliche Kommunikation offensichtlich nicht möglich. Wird hingegen eine sichere Verschlüsselungsmethode entwickelt, dann bedeutet diese architektonische Entscheidung im Code, dass Strafverfolgungsbehörden aufgrund der mathematischen Grundlagen keinen *einfachen Fernzugriff* auf die vertrauliche Kommunikation haben können.[85] Auch für die Identifikation gilt: Wenn die Nutzung eines Produkts nur nach einer Identifizierung möglich ist, handelt es sich um eine Zugriffsbeschränkung aufgrund der Architektur respektive des Codes.[86]

Jede dieser vier Modalitäten beeinflusst, wie eine Gesellschaft mit verschlüsselter Kommunikation respektive Identifikation umgehen kann. Damit kommen wir zur zweiten Frage (2) dieses Abschnitts: Auf welchem Weg könnte das Ziel einer Reduktion frei verfügbarer und verschlüsselter Kommunikation (oder die Verpflichtung zur Identifikation) über Intermediäre erreicht werden? In unserem Beispiel dürfte sich die Legislative darüber im Klaren sein, dass ein *direktes* Verbot der Kryptographie zwar bei entsprechend schwerer Strafandrohung erfolgversprechend sein könnte, allerdings würde eine solche Methode zu größeren Protesten und schwerwiegenderen rechtlichen Problemen führen. Es würde wahrscheinlich zu scharfer Kritik kommen, wenn Menschen allein wegen der Nutzung von Kryptographie in der interpersonellen Kommunikation mit harten Strafen zu rechnen hätten. Jeder Einzelne und jede Einzelne würde zwar wissen, dass verschlüsselte Kommunikation ab sofort verboten wäre,

85 *Fernzugriff* (engl. *remote access*) bedeutet hier, dass die Kommunikation von einem entfernten Ort und ohne direkten Zugriff auf die Endgeräte mitgelesen werden kann. Ein direkter Zugriff auf Endgeräte ermöglicht den Strafverfolgungsbehörden in vielen Fällen trotzdem ein Auslesen der Kommunikation. Darauf wird Teil III zurückkommen.

86 Siehe Lessig, *Code*, S. 124–125.

dieser Eingriff wäre in unserem Gedankenspiel nach Meinung der Gesetzgeber jedoch nicht zu vertreten und unverhältnismäßig.[87]

Die mögliche Alternative ist nun, mit *indirekter* Regulierung die Intermediäre zu bestimmten Aktionen zu verpflichten. Diese Intermediäre würden angewiesen werden, nur eine solche „vertrauliche" Kommunikation zu ermöglichen oder zu entwickeln, bei der staatliche Institutionen in bestimmten Fällen auch *remote* und *per Fernzugriff* auf diese Kommunikationsinhalte zurückgreifen können.[88] Hinzu käme, dass diese Reduktion der Vertraulichkeit nur für den Eingriff von Strafverfolgungsbehörden möglich sein soll, nicht aber für andere, böswillige Parteien.[89] In der Systematisierung von Regulierung würde das bedeuten: Vertrauliche Kommunikation wird indirekt mithilfe von Code und Intermediären gesteuert. Äquivalent ist dies auch auf das Gebot der Identifikation anwendbar.

Die konkrete Ausgestaltung indirekter Regulierung kann unterschiedlichste Intermediäre und Technologien betreffen. Erfolgen würde sie entweder über eine Einflussnahme auf die wissenschaftliche Entwicklung und Standardisierung von sicherer Kryptographie (etwa durch reduzierte Schlüssellängen), mit einer geographischen Beschränkung der Distribution (etwa durch Exportrestriktionen), mit implementierten Backdoors in verkaufter Software (etwa mit einer Schlüsselhinterlegung in den Datenbanken der Strafverfolgungsbehörden) oder über ein sogenanntes Client-Side-Scanning (etwa eine automatische Analyse von Bildern auf den Endgeräten zur Detektion von strafbarem Material). All diese Versuche haben unterschiedliche Vor- und Nachteile. Teil III wird argumentieren, dass in *allen* Fällen die Nachteile aus technologischer wie ethischer Perspektive überwiegen. Außerdem wird in Abschnitt 8.2 ein Framework vorgestellt, das eine indirekte Regulierung im Kontext möglicher Grund- und Menschenrechtsverletzungen ethisch-normativ bewertet.

Um eine solche Analyse aber zu ermöglichen, lohnt sich eine genauere Einordnung der verschiedenen Optionen der Regulierung. Diese Einordnung erfolgt historisch-systematisch anhand der Beispiele der seit den 1960er-Jahren stattfindenden Crypto Wars. *Historisch* bedeutet,

87 Was nicht bedeutet, dass andere Eingriffe deswegen verhältnismäßig wären.

88 Als Beispiel kann hier Senate Bill 266 dienen; siehe Abschnitt 3.1.

89 Dass Letzteres technologisch schwer umzusetzen ist, tut an dieser Stelle nichts zur Sache.

dass diese Beispiele auch tatsächlich vorgeschlagen wurden. *Systematisch* meint, dass es sich hierbei aber nicht um eine chronologische Aufzählung handelt, sondern um eine Einordnung anhand von Lessigs Modalitäten und der Möglichkeiten der Regulierung mithilfe von Intermediären. Wir werden uns dabei auf die vier bereits genannten Vorschläge beschränken, die geschichtlich vorwiegend in den USA diskutiert wurden.[90] Diese vier Arten der Regulierung sind: Beeinflussung der Forschung, Exportbeschränkungen, Backdoors und Client-Side-Scanning.[91]

Beeinflussung der Forschung

Für Craig Jarvis lässt sich der Beginn der Crypto Wars auf Kahns *The Codebreakers* zurückführen: Nach Ansicht von James Bamford gelangte Kahn in den 1960er-Jahren durch seine Arbeit auf die Beobachtungsliste der NSA, wodurch seine Telefongespräche und Telegramme abgehört werden konnten.[92] Neben der Überwachung Kahns kam eine Einflussnahme der NSA auf den Macmillan Verlag hinzu.[93] Die Methodiken schlugen letztlich fehl, sind aber ein Beispiel dafür, wie über einen Intermediär wie den Macmillan Verlag eine Regulierung erfolgen sollte.

Der damit *erste* Crypto War handelte also von Diskussionen um akademische Freiheit, später auch von der Standardisierung kryptographischer Protokolle.[94] Ausgetragen wurde dieser Disput von der NSA einerseits und Forschenden andererseits. Ein bedeutender Intermediär,

90 Die Gründe hierfür sind abermals historisch bedingt, insofern die kryptographische Forschung in den 1960er- und 1970er-Jahren zum allergrößten Teil in den USA stattfand, weshalb die Reaktion des US-amerikanischen Staates nicht lange auf sich warten ließ. Hinzu kommt, dass die USA mit der NSA über einen mächtigen Geheimdienst verfügen, der in den 1960ern und später ein Monopol im Bereich der kryptographischen Forschung beanspruchte. Siehe weiterführend Kapitel 2.

91 Am aktuell bedeutendsten ist das Client-Side-Scanning, das Abschnitt 8.1 aus dediziert ethischer Perspektive beleuchten wird.

92 Siehe James Bamford. *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*. Harmondsworth: Penguin Books, 1983, S. 169; zitiert und diskutiert in Jarvis, *Crypto Wars*, S. 72, allgemeiner auch S. 72–73.

93 Siehe Bamford, *The Puzzle Palace*, S. 171, zum Kontext auch S. 171–173; diskutiert in Jarvis, *Crypto Wars*, S. 73.

94 Vor allem bezogen auf DES; siehe ebd., S. 78–90. Weiterführend ist auch der Fall um den NSA-Mitarbeiter Joseph A. Meyer interessant, für den allerdings auf die Literatur verwiesen sei; siehe einführend etwa Bauer, *Secret History*, S. 423–430.

der für die NSA dabei eine Rolle spielte, war die *National Science Foundation* (NSF), von der Forschende finanzielle Unterstützung erhielten.[95] Genauso wie der Versuch, kryptographische Forschung zu klassifizieren, stellte sich dies jedoch weitgehend als Misserfolg heraus.[96] Das Verhältnis von NSA und Forschenden mündete schließlich in einem freiwilligen Review-System, das mit einem globalen Internet jedoch bald an Effizienz verlieren musste.[97]

Eine andere Möglichkeit zur Beeinflussung der Forschung war das *National Bureau of Standards* (NBS), das spätere *National Institute of Standards and Technology* (NIST). Dabei wurden bei der Standardisierung des *Data Encryption Standard* (DES) Entscheidungen getroffen, die auf einen entscheidenden Einfluss der NSA hindeuteten.[98] IBM als Entwickler von *Lucifer* und die NBS kooperierten schließlich mit der NSA – ein prägnantes Beispiel für die Modalität des Marktes in Verbindung mit staatlicher Regulierung. So wurde etwa IBM von der NSA überzeugt, dass die 56-Bit-Schlüssellänge ausreichend sei.[99] Zu betonen ist hierbei, dass die Anzahl möglicher Schlüssel mit jedem Bit verdoppelt wird. Unter anderem aufgrund des 56-Bit-Schlüssels gilt DES heute als nicht mehr sicher, konnte doch bereits im Jahr 1997 eine mit DES verschlüsselte Nachricht im Rahmen des *DESCHALL*-Projekts entschlüsselt werden.[100]

Zu weitreichender Kontroverse führte auch die Entscheidung der NSA, die Designprinzipien der sogenannten *Substitutionsboxen* (*S-Boxen*) bei DES nicht zu veröffentlichen. Wie bereits in Abschnitt 2.2 beschrieben, beruhte diese Entscheidung zwar wahrscheinlich nicht auf der Verheimlichung einer Backdoor; allerdings entschloss sich die NSA aus einem anderen Grund zur Geheimhaltung der S-Boxen: Der NSA respektive IBM war eine neuartige Methode zur Kryptoanalyse bekannt, die sogenannte *Differentielle Kryptoanalyse*, wobei die S-Boxen diese Kryptoanalyse erfolgreich verhindern konnten. Da die NSA sich zur Geheimhaltung der neuartigen Technik entschieden hatte, wurde diese Art der Krypto-

95 Siehe dazu und zum Folgenden Jarvis, *Crypto Wars*, S. 129–132. Beispielsweise profitierten von der NSF auch Whitfield Diffie und Martin Hellman; siehe ebd., S. 130.

96 Siehe umfassender ebd., S. 131–144.

97 Siehe ebd., S. 141–144 sowie S. 147–148.

98 Siehe Levy, *Crypto*, S. 59.

99 Siehe United States Senate, *Unclassified Summary*, S. 4; weiterführend auch Abschnitt 2.2.

100 Siehe zu DES ausführlicher Abschnitt 2.2; zum DESCHALL-Projekt einführend Jarvis, *Crypto Wars*, S. 95–97.

analyse erst 1991 von den Kryptographen Biham und Shamir öffentlich beschrieben.[101]

Mit späteren Standardisierungen wie etwa AES nahm auch die Bedeutung einer Beeinflussung der Forschung sukzessive ab. Die kommerziellen und technologischen Gründe (wie etwa Kerckhoffs' Prinzip) sind bereits in Abschnitt 2.2 diskutiert worden. Hinzu kam nun aber, dass Informationen und kryptographische Standards über das Internet verbreitet werden konnten und Kryptographie zunehmend zivil, global und kommerziell notwendig wurde. Eine Beeinflussung oder gar Klassifizierung von Forschungsleistung konnte nunmehr selbst zum Sicherheitsrisiko werden. Bereits dieser erste Crypto War zeigt konzeptuell, wie eng die Moderne Kryptographie mit gesellschaftlichen und politischen Entscheidungen verbunden ist.

Exportbeschränkungen

Bei Exportbeschränkungen handelt es sich um den Versuch, die Distribution von kryptographischen Anwendungen, Algorithmen oder Implementierungen ins Ausland zu verhindern. Kryptographie wurde dazu als *Munition* oder als *Dual-Use-Technologie* klassifiziert.[102] *Dual-Use* bedeutet in diesem Zusammenhang, dass eine Technologie sowohl für militärische als auch für kommerzielle oder zivile Zwecke genutzt werden kann. Die US-amerikanischen Exportbeschränkungen waren daher vor allem auch ein Konflikt zwischen den Interessen der Geheimdienste auf der einen und den ökonomischen Zielen der Industrie auf der anderen Seite.

Neben diesem Disput von Geheimdiensten und Industrie waren an den US-amerikanischen Crypto Wars aber auch sehr bald Cryptoaktivistinnen und -aktivisten beteiligt, die die Schwierigkeiten und Widersprüchlichkeiten dieser Dual-Use-Klassifikation aufzeigen wollten. So veröffentlichte etwa das MIT eine gedruckte Version der PGP-Software

101 Siehe Eli Biham und Adi Shamir. „Differential Cryptanalysis of DES-like Cryptosystems". In: *Journal of Cryptology* 4.1 (1991), S. 3–72; siehe auch Coppersmith, „The Data Encryption Standard (DES) and its strength against attacks"; zu diesem Absatz allgemeiner Levy, *Crypto*, S. 55–56.

102 Siehe dazu und zu diesem Absatz einführend Diffie und Landau, *Privacy on the Line*, S. 120–123, sowie Thea Riebe. *Technology Assessment of Dual-Use ICTs: How to Assess Diffusion, Governance and Design*. Wiesbaden: Springer Vieweg, 2023; weiterführend außerdem Abschnitt 6.1.

in Form eines Buches.[103] Was würde passieren, wenn sich Zimmermann und das MIT nun um eine Ausfuhrgenehmigung beim State Department bemühen würden? Ließe sich der Export eines 600-Seiten-Buches mit tausenden Zeilen Code verhindern?[104] Tatsächlich erhielten sie auf ihre Anfrage im Jahr 1995, ob dieses Buch unter die Exportbeschränkungen fallen würde oder nicht, zunächst keine Antwort, worauf sie es in einer Auflage von 1.500 Exemplaren veröffentlichten.[105] An der Universität Bremen wurde wenige Zeit später das gesamte Werk eingescannt und auf einen Server geladen, sodass ein globaler und legaler Zugriff darauf möglich wurde.[106] Die Exportbeschränkungen waren damit umgangen.

Auf ähnliche Weise zeigt auch die Idee von Phil Karn die Problematik und Widersprüchlichkeit von Exportbeschränkungen.[107] Karn bat das State Department um Exporterlaubnis für Bruce Schneiers bekanntes Buch *Applied Cryptography*, das unter anderem den Quellcode von DES abgedruckt hatte. In dieser Buchform wurde die Erlaubnis erteilt. Danach sendete Karn eine weitere Anfrage, dieses Mal waren die kryptographischen Algorithmen jedoch auf einer Diskette digitalisiert. Nach längerer Wartezeit lehnte das State Department diesen Export ab. Darauf folgte ein Rechtsstreit, bis schließlich die Clinton-Regierung die Exportbeschränkungen liberalisierte und die Diskette nicht mehr unter die Regulierung fiel.[108]

Ein letztes Beispiel stellt Daniel Bernsteins Algorithmus *Snuffle* dar.[109] Dieser Algorithmus war zwar keine Verschlüsselungsfunktion, jedoch war er geeignet, eine Hashfunktion zu einem solchen Verschlüsse-

103 Siehe Diffie und Landau, *Privacy on the Line*, S. 230; ausführlicher auch Jarvis, *Crypto Wars*, S. 230–233. Zu dem genannten Buch siehe Phil Zimmermann. *PGP: Source Code and Internals*. Cambridge, MA: MIT Press, 1995.

104 In diesem Fall ging es um die *International Traffic in Arms Regulations* (ITAR).

105 Siehe Jarvis, *Crypto Wars*, S. 230 sowie S. 232. Am Tag der Veröffentlichung erhielten sie einen Anruf vom State Department, in dem ihnen mitgeteilt wurde, dass das Buch nicht unter die ITAR fallen würde – die NSA hätte wohl das Gegenteil empfohlen. Siehe ebd., S. 230–231.

106 Siehe ebd., S. 232.

107 Siehe zu Phil Karn, den betreffenden Exportanfragen und zu diesem Absatz Greenberg, *This Machine Kills Secrets*, S. 86–87; siehe auch Diffie und Landau, *Privacy on the Line*, S. 121–122.

108 Siehe weiterführend zu Phil Karn und den genannten Exportbeschränkungen Jarvis, *Crypto Wars*, S. 257–266.

109 Siehe dazu und zu diesem Absatz umfassender ebd., S. 238–257; siehe im Kontext des Cryptoaktivismus auch Abschnitt 3.2.

lungssystem zu modifizieren.[110] Im Jahr 1992 wollte Bernstein den Algorithmus schließlich veröffentlichen und stellte dazu die Anfrage, ob seine Software unter die Exportrestriktionen falle.[111] William B. Robinson, Direktor des *Office of Defense Trade Controls*, antwortete Bernstein, dass dazu eine Exportlizenz notwendig sei.[112] Bernstein gab sich mit der Antwort Robinsons nicht zufrieden und forderte gemeinsam mit Bürgerrechtsorganisationen und unter öffentlichem Druck die Exportbeschränkungen heraus.[113] Im folgenden juristischen Prozess gewann Bernstein sowohl im *Northern California District Court* als auch im *Court of Appeals for the Ninth Circuit*.[114] Die Bedeutung dieses Falles fasst Craig Jarvis wie folgt zusammen:

> Bernstein's case had been one of the most consequential in history – it had forced a judicial reckoning of the constitutionality of the export regulations which had resulted in the recognition of encryption as an expression of free speech and forced severe concessions in the regulations.[115]

Backdoors

Im Falle der Ende-zu-Ende-Verschlüsselung (E2E-Verschlüsselung) ist ein *einfacher Fernzugriff* auf Nachrichten weder durch den Betreiber (z. B. eines Messengerdienstes) noch eine sonstige Drittpartei (z. B. eine Strafverfolgungsbehörde) möglich. Selbst im Falle eines Gerichtsbeschlusses könnte der Markt (also der Betreiber des Messengers) nicht dazu verpflichtet werden, die Nachricht eines möglichen Verdächtigen per Fernzugriff zu entschlüsseln, insofern eine E2E-Verschlüsselung dies verhindert.[116]

Unter anderem solche Argumente führten zu der Idee, Intermediäre zu einer sogenannten *Backdoor* (dt. *Hintertür*) oder zu einem *Key Escrow*

110 Siehe Jarvis, *Crypto Wars*, S. 239.
111 Siehe Levy, *Crypto*, S. 298.
112 Siehe Jarvis, *Crypto Wars*, S. 240.
113 Siehe Levy, *Crypto*, S. 300–302.
114 Siehe Diffie und Landau, *Privacy on the Line*, S. 255, sowie Levy, *Crypto*, S. 300; weiterführend Dame-Boyle, *EFF at 25*.
115 Jarvis, *Crypto Wars*, S. 257.
116 Ein direkter Zugriff über die Endgeräte der Kommunikationspartner kann zwar mit höherer Wahrscheinlichkeit erfolgreich sein, ist aber weniger praktikabel und erfordert einen größeren Aufwand.

(dt. *Schlüsselhinterlegung*) zu verpflichten.[117] Die grundsätzliche Idee dabei ist, dass Strafverfolgungsbehörden unter bestimmten Umständen und mit einer Art *Umgehung* der E2E-Verschlüsselung Zugriff auf bestimmte Nachrichten erhalten sollen. Vereinfacht lässt sich das Vorgehen mit einem abschließbaren Schließfach für Schülerinnen und Schüler vergleichen: Nur die Schülerin oder der Schüler weiß die Kombination und kann das Schließfach öffnen.[118] Andere Schülerinnen und Schüler können dies nicht. Hinzu kommt nun aber, dass es noch eine weitere Möglichkeit gibt, das Fach zu öffnen: Über einen Generalschlüssel, den nur das Lehrkollegium besitzt. Backdoors zielen auf eine ähnliche Funktion ab.[119]

Im Falle einer verpflichtenden Implementierung einer Backdoor würde eine Regulierung über die Intermediäre erfolgen. Die dabei relevanten Modalitäten sind einerseits der Markt (Verpflichtung zur Backdoor unter Strafandrohung) und andererseits der Code (Änderung der Architektur zur Implementierung einer Backdoor). Am bekanntesten wurde hier ein Versuch der US-amerikanischen Regierung: der sogenannte *Clipper-Chip*.[120] Die Intention dabei war, zwei scheinbar inkompatible Perspektiven zusammenzubringen: „the need for strong public codes and the agency's need for plaintext traffic"[121]. Zur Lösung des Pro-

117 Zahlreich zitiert wurde für die Kritik an solchen Methoden ein Artikel aus dem Jahr 1997, den einige führende Kryptographen verfasst hatten: Hal Abelson u. a. *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*. 27. Mai 1997. URL: https://doi.org/10.7916/D8GM8F2W (besucht am 15.04.2024); später auch Harold Abelson u. a. „Keys under doormats: mandating insecurity by requiring government access to all data and communications ‡". In: *Journal of Cybersecurity* 1.1 (2015), S. 69–79. Siehe zur Bedeutung dieses Artikels Webb, *Coding Democracy*, S. 144.

118 Diese Analogie ist beschrieben nach Diffie und Landau, *Privacy on the Line*, S. 7.

119 Backdoors können auch unbemerkt implementiert werden, wie etwa beim Algorithmus *Dual_EC_DRBG*, der 2006 durch die NIST standardisiert wurde. Nach der Veröffentlichung von internen NSA-Dokumenten durch Edward Snowden hatte es bei diesem Algorithmus wohl tatsächlich eine Backdoor für die NSA gegeben. Siehe Nicole Perlroth. „Government Announces Steps to Restore Confidence on Encryption Standards". In: *New York Times* (10. Sep. 2013). URL: https://archive.nytimes.com/bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/ (besucht am 15.04.2024); einführend auch Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 274.

120 Siehe einführend Levy, *Crypto*, S. 226–268; umfassender Jarvis, *Crypto Wars*, S. 157–210; zudem auch Anderson, *Security Engineering*, S. 928–931, sowie Rid, *Rise of the Machines*, S. 273–276.

121 Levy, *Crypto*, S. 229.

blems kam dem NSA-Mitarbeiter Clinton Brooks eines Nachts die entscheidende Idee, die Steven Levy wie folgt beschreibt:

> There *could* be a compromise that could satisfy everybody. In the physical world, a search warrant compelled a suspect in a crime to give authorities the combination of a safe. Why not translate that concept to the world of communications and computers? If you created a system by which special duplicate encryption keys were somehow spirited away and stored in secure facilities, you would essentially be holding lock combinations *in escrow*, unavailable to anyone but those who had authority to retrieve them.[122]

Brooks wollte damit bewusst eine nationale Debatte über den Umgang mit Kryptographie anstoßen, obschon dies von der NSA argwöhnisch beäugt wurde.[123] Als kryptographischer Algorithmus wurde der durch die NSA entwickelte *Skipjack* ausgewählt, der mit einer 80-Bit-Schlüssellänge eine deutlich höhere Sicherheit bieten sollte als der damals noch geltende DES.[124] Genauere Implementierungsdetails sind an dieser Stelle nicht relevant, das zentrale Element allerdings war das sogenannte *Law Enforcement Access Field* (LEAF). Mithilfe der Informationen des LEAF sollte es Behörden möglich sein, auf einen in einer sicheren Datenbank gespeicherten Schlüssel zurückgreifen zu können.[125] Da *nur* Behörden darauf Zugriff hätten, sollte die Kommunikation für andere Drittparteien weiterhin verschlüsselt sein.[126]

Mit diesem Beispiel können wir nun systematisieren, wie Regulierung von Kryptographie erfolgen kann. Backdoors können durch den Einfluss des Gesetzgebers auf verschiedene Arten verbreitet werden. Einerseits wäre ein gesetzliches Verbot anderer Kryptographie naheliegend.[127] Andererseits wäre eine weitere Möglichkeit, per Subventionierung die Anreize zu erhöhen, durch die der Markt – je nach Definition von Freiheit – *freiwillig* zur staatlich implementierten Backdoor greifen würde.[128]

122 Levy, *Crypto*, S. 230, kursiv im Original.
123 Siehe ebd., S. 230–231.
124 Siehe dazu und zur folgenden Beschreibung des LEAF ebd., S. 232.
125 Tatsächlich sollte der Schlüssel getrennt werden, um ihn in zwei Datenbanken an unterschiedlichen Orten zu speichern; siehe ebd., S. 234.
126 Die NIST genehmigte am 9. Februar 1994 den *Escrowed Encryption Standard* als *Federal Information Processing Standard* (FIPS). Siehe auch Diffie und Landau, *Privacy on the Line*, S. 237–238.
127 Siehe im Kontext des Clipper-Chips Lessig, *Code*, S. 66–67.
128 Siehe ebd., S. 66–67.

Im Kontext des Clipper-Chips waren Letzteres nach Levy „considerable carrots“ [129], welche die Bundesbehörden dem Telekommunikationsunternehmen *AT&T* anzubieten hatten: erstens die Tatsache, dass Skipjack zumindest für Drittparteien schwerer zu brechen war als DES; zweitens die Möglichkeit, solche Telefongeräte wahrscheinlich auch ins Ausland exportieren zu dürfen; und drittens die Aussicht darauf, dass die Behörden Tausende dieser Telefone kaufen würden. [130]

Trotz dieser Anreize war die Reaktion von anderen Unternehmen, Forschenden und der Gesellschaft außergewöhnlich ablehnend, und alle Versuche, den Clipper-Chip zu etablieren, scheiterten letztlich aus überzeugenden Gründen. [131] Abgesehen von den technischen Schwächen und der Reduktion von Privacy gab es für Unternehmen außer jenen künstlichen Anreizen keine Vorteile. [132] Die Implementierung des Clipper-Chips sorgte für zusätzliche Kosten, vor allem aber konnte *nur* die US-amerikanische Regierung auf diese Backdoor zugreifen. [133] Wer außerhalb der USA kauft ein Produkt, bei dem von vornherein klar ist, dass die US-amerikanische Regierung Zugriff darauf hat? [134]

Auch Lessig diskutiert in *Code: Version 2.0* explizit den Clipper-Chip im Rahmen einer Regulierung von Kryptographie. Während er darauf verweist, dass der Clipper-Chip weder durch ein Verbot anderer Kryptographie noch durch Subvention einen Erfolg verbuchen konnte, nennt er eine weitere Möglichkeit: die *direkte* Regulierung der Entwicklung von Kryptographie. Dabei müsse für die Entwicklerinnen und Entwickler von Softwarecode die Bedingung gelten, dass sie eine Backdoor in den betreffenden Code implementieren, durch den Regierungen einen Zugriff erhalten können. [135]

Lessig führt drei Argumente an, die im Vergleich zu Verboten und Subventionen für eine solche Regulierung sprechen würden. [136] Erstens

129 Levy, *Crypto*, S. 237.

130 Siehe ebd., S. 237.

131 Siehe dazu Diffie und Landau, *Privacy on the Line*, S. 236–237; darüber hinaus auch Levy, *Crypto*, S. 303, sowie Blaze, „Protocol Failure in the Escrowed Encryption Standard“.

132 Zu den technischen Schwächen siehe ebd.; zu aktuelleren technischen Problemen solcher Methoden insbesondere auch Abelson u. a., „Keys under doormats“.

133 Siehe Diffie und Landau, *Privacy on the Line*, S. 7–8.

134 Siehe ebd., S. 8.

135 Siehe Lessig, *Code*, S. 66.

136 Siehe dazu und zu diesem Absatz ebd., S. 67.

würde diese Art der Regulierung nicht das Recht des Individuums auf verschlüsselte Kommunikation betreffen. Es würden nur die verfügbaren kryptographischen Technologien reguliert. Als Vergleich verweist Lessig auf Autos, wo die Herstellung reguliert sei. Zweitens würde eine solche Regulierung weiterhin Marktteilnehmern einen Anreiz bieten, um die besten kryptographischen Verfahren zu konkurrieren. Und drittens würde es sich nur um eine geringe Anzahl an Herstellern handeln, die reguliert werden müssten. Für Lessig bedeutet dies zusammenfassend:

> [T]his solution is an example of the government regulating code directly so as to better regulate behavior indirectly; the government uses the architecture of the code to reach a particular substantive end.[137]

Üblicherweise kann eine solche Regulierung auch dahingehend formuliert werden, dass der Gesetzgeber die Hersteller und Betreiber von Kommunikationsdienstleistungen verpflichtet, einen Zugriff auf Klartextnachrichten für Strafverfolgungsbehörden zu ermöglichen. Ein Beispiel wäre hier der bereits bei PGP diskutierte Senate Bill 266.[138] Für Marktteilnehmer ergeben sich dadurch lediglich zwei Möglichkeiten, um weiterhin straffrei am Markt partizipieren zu können: (1) entweder eine Verschlüsselung zur vertraulichen Kommunikation generell nicht mehr anzubieten, was jedoch marktwirtschaftlich unklug wäre, (2) oder eben eine Backdoor zu implementieren.[139]

Normativ betrachtet sind solche *indirekten* Vorschläge zu kritisieren, wie Abschnitt 8.2 analysieren wird. Zudem ist die konkrete Umsetzung solcher Gesetze diskussionswürdig, wie das Beispiel von Senate Bill 226 historisch zeigen konnte. Und auch der Clipper-Chip scheiterte letztlich aus technologischen und politischen Gründen. Unabhängig von diesen normativen Fragen sind Backdoors gegebenenfalls aber eine *Möglichkeit* der Beschränkung und Regulierung von Kryptographie, die unterschiedliche Intermediäre und Modalitäten betreffen kann.

137 Lessig, *Code*, S. 67.
138 Siehe Levy, *Crypto*, S. 195–196, sowie Abschnitt 3.1.
139 Siehe im Kontext von Senate Bill 266 ebd., S. 196.

Client-Side-Scanning

Das Client-Side-Scanning (CSS) kann topologisch als eine Unterkategorie von Backdoors betrachtet werden. Verglichen mit den bisherigen Arten der Regulierung ist das CSS dabei die neueste – gewissermaßen auch *innovativste* – Möglichkeit zur Einschränkung vertraulicher Kommunikation.[140] Wie der Name des CSS bereits andeutet, handelt es sich grundsätzlich um einen Scanvorgang aufseiten der Clients, in diesem Fall also der Endgeräte. Ein *Client* ist per definitionem ein Programm, ein Gerät oder ein Dienst, der wiederum die Dienstleistung eines *Servers* in Anspruch nimmt.[141] Vereinfacht können wir uns hier als Client ein Smartphone vorstellen und als Server den Messenger-Server, mit dem das Smartphone kommuniziert.[142] Eine Nachricht von Alices Smartphone an Bobs Smartphone wird über den Server geleitet. Die Nachrichten können dabei zwar serverseitig gespeichert werden, eine Ende-zu-Ende-Verschlüsselung ist jedoch dann gewährleistet, wenn die Nachricht ab dem Versenden auf Alices Smartphone bis zum Empfang auf Bobs Smartphone verschlüsselt ist. Auch der Server hat also keine Möglichkeit, den unverschlüsselten Text einer Nachricht auszulesen.

Das Innovative am CSS ist nun, dass der Scanvorgang nicht auf dem Server, sondern auf dem Client-Gerät (z. B. dem Smartphone) stattfindet – also *vor* der Verschlüsselung und *bevor* die Nachricht das Client-Gerät verlässt.[143] Das Scanning erfolgt anhand bestimmter Kriterien, sodass etwa eine Nachricht, die möglicherweise einen Drogenhandel zum In-

140 Siehe zur Einführung Internet Society. *Client-Side Scanning: What It Is and Why It Threatens Trustworthy, Private Communications*. Aug. 2022. URL: https://www.internetsociety.org/wp-content/uploads/2020/03/2022-Client-Side-Scanning-Factsheet-EN.pdf (besucht am 15.04.2024).

141 Dieses grundlegende Konzept von Netzwerken wird auch als *Client-Server-Modell* bezeichnet. Siehe z. B. Jin Jing, Abdelsalam Sumi Helal und Ahmed Elmagarmid. „Client-server computing in mobile environments". In: *ACM Computing Surveys* 31.2 (1999), S. 117–157; einführend auch Alok Sinha. „Client-server computing". In: *Communications of the ACM* 35.7 (1992), S. 77–98.

142 In der Realität kann ein Server aber gleichzeitig auch ein Client sein, wenn er beispielsweise andere Dienste von einem weiteren Server in Anspruch nimmt. Damit kann auch ein Client gleichzeitig als Server dienen. Für die folgenden Ausführungen ist eine weitere Präzisierung jedoch nicht notwendig.

143 Für eine Einführung und Darstellung des CSS sowie zum Folgenden siehe Hal Abelson u. a. *Bugs in our Pockets: The Risks of Client-Side Scanning*. 2021. arXiv: 2110.07450. URL: https://arxiv.org/abs/2110.07450 (besucht am 15.04.2024); sowie Internet Society, *Client-Side Scanning*.

halt hat, als *möglicherweise illegal* gekennzeichnet werden kann.[144] Diese Nachricht würde anschließend an eine Drittpartei, etwa eine Strafverfolgungsbehörde, weitergeleitet werden. Die konkrete Umsetzung und die Kriterien zur Klassifikation von Nachrichten können hierbei variieren. Aktuelle Gesetzesvorschläge betreffen unter anderem sogenanntes *Grooming*, was einen missbräuchlichen Anbahnungsversuch an Minderjährige durch Erwachsene beschreibt.[145]

In der Systematik der Regulierung kann der Gesetzgeber beim CSS ähnlich wie bei Backdoors darauf abzielen, Kommunikationsdienstleister zu einer solchen Implementierung zu verpflichten. Dies könnte zum Beispiel durch Strafandrohung oder die Verknüpfung an Lizenzaufträge erfolgen. Wenn sich ein Dienstleister weigert, ein solches Scanning zu implementieren, müsste er damit rechnen, den Markt verlassen zu müssen. Es handelt sich damit erneut um eine Regulierung mithilfe von Intermediären. Das Recht zielt darauf ab, die Modalität des Marktes (Dienstleister von Kommunikation) sowie die Modalität des Codes (implementiertes CSS) zu steuern und zu beeinflussen.

Normativ betrachtet mag es auf den ersten Blick so scheinen, als würde das CSS einerseits eine möglichst geringe Privacy-Verletzung versprechen, andererseits aber eine möglichst erfolgreiche Strafverfolgung zur Folge haben. Kritikerinnen und Kritiker hingegen monieren, dass das CSS trotz aller vermeintlichen Versprechen einen *faktischen* Bruch der Ende-zu-Ende-Verschlüsselung zur Folge hat und als Schwachstelle von böswilligen Parteien ausgenutzt werden kann.[146] Abschnitt 8.1 wird diese und weitere (Gegen-)Argumente kritisch untersuchen.

Zusammenfassend hat dieses Kapitel deutlich gemacht, dass eine Regulierung von Kryptographie möglich ist – entgegen den Hoffnungen und Vorstellungen mancher Cypherpunks. Eine solche Regulierung war zwar

144 Zum Beispiel mittels eines Vergleichs der Hashwerte von Nachrichten oder per maschinellem Lernen. Siehe Abelson u. a., *Bugs in our Pockets*, S. 7–8.

145 Im Kontext der EU siehe European Comission. *Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. COM(2022) 209 final*. 2022. URL: https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF (besucht am 15.04.2024), zum Grooming auch S. 13–15; siehe zudem Abschnitt 8.1.

146 Siehe ausführlicher zur Kritik Abelson u. a., *Bugs in our Pockets*, sowie Abschnitt 8.1.

historisch betrachtet oftmals begleitet von konsequentialistischen Kollateralschäden (z. B. bei Backdoors) oder logischen Widersprüchlichkeiten (z. B. bei Exportbeschränkungen). Gleichwohl bleibt die generelle Möglichkeit einer Regulierung der Anwendung von Kryptographie bestehen, bei der die *Mehrheit* der Menschen indirekt und per Intermediäre betroffen ist. Mit einer Synthese der technologischen Grundlagen aus Teil I und der gesellschaftlichen Aspekte aus Teil II kann nun Teil III auch aus normativ-ethischer Perspektive analysieren, ob eine solche Regulierung und Einschränkung von Kryptographie geboten ist.