Laurence Lerch

Ethik der Kryptographie

Nomos

Ethik | Ethics

herausgegeben von | edited by

Prof. Dr. Peter G. Kirchschläger
Prof. Dr. Christine Abbt
Prof. Dr. Georges Enderle

Band | Volume 3

Laurence Lerch

Ethik der Kryptographie

Nomos

Gefördert durch die Hanns-Seidel-Stiftung aus Mitteln des deutschen Bundesministeriums für Bildung und Forschung. Publiziert mit Unterstützung des Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

1. Auflage 2025

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

Zugl.: Luzern, Universität, Diss., 2024

ISBN (Print): 978-3-7560-3158-0
ISBN (ePDF): 978-3-7489-5500-9

DOI: https://doi.org/10.5771/9783748955009

Onlineversion
Nomos eLibrary

Danksagung

Die Universität Luzern hat die vorliegende Arbeit im Frühjahrssemester 2024 als Dissertation angenommen. Literatur und Forschung ist dementsprechend bis April 2024 berücksichtigt. Die vorangegangenen drei Jahre des unermüdlichen Forschens behalte ich als lehrreiche, aber auch entbehrungsreiche Zeit in Erinnerung, in der ich viel auf die Unterstützung meines akademischen und persönlichen Umfelds angewiesen war. Zunächst danke ich meinem Betreuer Prof. Dr. Peter G. Kirchschläger und dem Institut für Sozialethik an der Universität Luzern. Dort habe ich einen Platz gefunden, wo ich eigenständig denken, arbeiten und lernen durfte. Auch meinem Zweitgutachter Prof. Dr. Christian Preidel gebührt ein solcher Dank.

Inhaltlich möchte ich mich zudem bei all jenen Menschen bedanken, die sich seit Jahren unermüdlich für die Weiterentwicklung und die Verbreitung von Kryptographie einsetzen – sei es in der Wissenschaft, der Gesellschaft, der Politik oder den Medien. Ich denke hier zum einen an all jene, die sich als Cypherpunks identifizieren, zum anderen aber auch an die unzähligen Organisationen weltweit, die sich für Privatsphäre, Datenschutz und freie Meinungsäußerung engagieren. Ihr seid es, die mich zu diesem Forschungsthema gebracht haben.

Für dieses Unterfangen unerlässlich war aber auch die Fürsorge meiner Familie und Freunde. Dies nicht nur in den Jahren des intensiven Forschens, sondern vielmehr in all den vorherigen Kinder- und Jugendjahren, in denen sie mir stets den Raum zum Lernen und zur eigenen Entfaltung gegeben haben. Meinen beiden Eltern, meinen Großeltern aus Greding und Donauwörth, meiner Patentante sowie meinen sechs Geschwistern gilt dieser Dank ebenso wie Anke, die mich immer auf diesem Weg begleitet und die Arbeit in unzähligen Stunden Korrektur gelesen hat.

Inhaltsverzeichnis

Teil III Kryptographie & Ethik

Einführung

Mit dem Einzug von Verschlüsselungsmethoden in Smartphones, Laptops und das alltägliche Leben wandelte sich auch die Kryptographie als dahinterstehende Wissenschaft zum Politikum. Eine freie, zugängliche und tatsächlich genutzte Kryptographie ist das, wovor sich viele derer, die von unverschlüsselter Kommunikation profitieren, nur fürchten konnten. Politische Diskussionen über eine Beeinflussung kryptographischer Forschung, internationale Exportbeschränkungen oder sogenannte *Backdoors* für einen Zugriff auf vertrauliche Kommunikation waren die Folge. Der jüngste Angriff auf eine ubiquitäre Kryptographie ist eine Technologie, die im deutschsprachigen Raum unter dem Begriff der *Chatkontrolle* bekannt geworden ist: das Scannen von Nachrichten und Daten auf den Endgeräten der Nutzerinnen und Nutzer, genannt *Client-Side-Scanning*.

Diese politischen Diskussionen werden in den folgenden Kapiteln immer wieder aufgegriffen werden. Doch ist die Kryptographie weit mehr als nur ein Politikum. Vielmehr ist sie, so wird diese Arbeit argumentieren, eine *technologische*, *gesellschaftliche* und vor allem *ethische* Angelegenheit. Als Wissenschaft der Verschlüsselung und als Teil der Informationssicherheit findet sie im 21. Jahrhundert Anwendung in Technologien wie dem Internet. Gleichwohl ist Kryptographie aber auch mehr als nur eine nihilistische oder deterministische Wissenschaft und Technologie, erlaubt sie es doch Individuen, vertraulich und privat zu kommunizieren. Diese Möglichkeit führt allerdings zu gesellschaftlichen und sozialen Konsequenzen. Die Ethik ist es schließlich, die diese Verbindung von technologischen und gesellschaftlichen Facetten kritisch untersuchen soll. Denn die Frage ist bei alledem: *Wie sollen wir eigentlich mit Kryptographie umgehen?*

Das Spektrum der möglichen Antworten könnte größer kaum sein. Die einen behaupten, dass wir diese verschlüsselte Kommunikation beschränken sollten. Es sei offensichtlich, dass die weitverbreitete Kryptographie das Handeln der Strafverfolgungsbehörden erschwere. Anderer wiederum sagen, dass wir Kryptographie nur teilweise regulieren sollten. Es sei natürlich gut, dass Verschlüsselung existiere – aber doch nicht für alles und für jeden. Wieder andere meinen, wir sollten den Einsatz von Kryptographie fördern. Schließlich mache sie unser digitales Leben

sicherer. Die vielleicht deutlichste Form einer Antwort ist die Ansicht, dass die Frage gar nicht gestellt werden müsse. Kryptographie sei reine Mathematik. Die Algorithmen seien da. Wir könnten den Umgang mit Kryptographie weder steuern noch dessen Nutzung verhindern.

Es ist das Ziel dieser Arbeit, solche Antworten auf ihre argumentative Überzeugungskraft hin zu untersuchen. Denn diese letztlich ethischen Diskussionen zum Einsatz und zur Regulierung von kryptographischen Anwendungen haben einschneidende Auswirkungen. So ist etwa ein globales Finanzsystem auf funktionierende Transaktionen angewiesen. Die Veröffentlichung oder das Verändern privater Gesundheitsdaten darf nicht möglich sein. Und in der persönlichen Kommunikation verlassen wir uns darauf, dass unsere Nachrichten und unser Austausch sicher sind. So wichtig wie die Kryptographie für den Alltag und die digitale Sicherheit ist, so wichtig ist damit die ethische Diskussion um ihren *richtigen* Einsatz.

Eine Ethik der Kryptographie, die jedoch die technologischen und gesellschaftlichen Rahmenbedingungen vernachlässigt, würde sich der Gefahr der Realitätsferne oder gar Beliebigkeit aussetzen. Die Diskussion solcher Themen erfordert somit eine technologische, gesellschaftliche *und* ethische Perspektive auf die Kryptographie. Die Struktur der Arbeit reflektiert diese Methodik. Teil I diskutiert das Verhältnis von Kryptographie und Technologie, Teil II behandelt die gesellschaftliche Perspektive und Teil III argumentiert schließlich normativ im Sinne einer Ethik der Kryptographie. Zur Einführung seien die drei Teile und ihre Kapitel im Folgenden kontextuell beschrieben.

Teil I bildet die systematische Grundlage mit einer technologischen Sicht auf die Kryptographie. Einerseits dient dies einer niederschwelligen Einführung in die teils komplexen Konzepte der Kryptographie. Andererseits schlägt dieses Kapitel die Brücke von der Technologie zur Ethik als Geisteswissenschaft. In diesem Sinne ist dieser Teil primär für Ethikerinnen und Ethiker relevant. Gleichwohl können auch Personen aus den Natur- und Technikwissenschaften nützliche Gedanken aus der Systematisierung der Kryptographie gewinnen. Üblicherweise wird die Kryptographie dazu in zwei historische Paradigmen unterteilt: in die *Klassische Kryptographie*, die in Kapitel 1 behandelt wird, und in die *Moderne Kryptographie*, die in Kapitel 2 diskutiert wird.

Die Klassische Kryptographie dominierte bis zur Mitte des 20. Jahrhunderts. Dabei stand eine solche Möglichkeit zur Verschlüsselung nur

den Mächtigen der Welt zur Verfügung. Sie war primär ein Mittel zur Geheimhaltung und selbst eine Art Geheimwissenschaft. Doch durch die Entwicklungen im letzten Jahrhundert löste die Moderne Kryptographie das veraltete Verständnis von Verschlüsselung ab: Die Beschäftigung mit Kryptographie wurde zur systematischen Wissenschaft. Heute ist sie Teil der Informationssicherheit und aus dem digitalen Zeitalter nicht mehr wegzudenken. Dabei findet sie mit Themen wie der asymmetrischen Kryptographie Antworten auf Probleme, die lange Zeit unlösbar schienen.

Teil II behandelt anschließend die Wechselwirkung von Kryptographie und Gesellschaft. Dieses Verhältnis ist bidirektional: Einerseits hat der Paradigmenwechsel hin zu einer ubiquitären Kryptographie gesellschaftlich-soziale Diskussionen zur Folge. Die Moderne Kryptographie wird dabei zur Grundlage für neue Utopien, Ideologien und Vorstellungen über die Gesellschaft. Dazu stellt Kapitel 3 die Software *Pretty Good Privacy*, den Cryptoaktivismus und die Cypherpunks vor. Einige dieser frühen Cryptoaktivistinnen und -aktivisten dachten, dass Kryptographie nicht reguliert werden *kann*.

Die andere Richtung der Wechselwirkung von Kryptographie und Gesellschaft zeigt aber in Kapitel 4, dass Kryptographie zumindest für die meisten Menschen regulierbar und beschränkbar ist. Mit einer Analogie zum frühen Internet und mit den wegweisenden Arbeiten von Lawrence Lessig sowie Jack Goldsmith und Tim Wu soll auf theoretischer Basis eruiert werden, auf welche Weise eine solche Regulierung funktionieren kann.[1] Dieses Kapitel wird damit darlegen, dass Kryptographie keine nihilistische Technologie mehr ist. Ganz im Gegenteil ist sie beeinflussbar durch politische, gesetzliche und rechtliche Rahmenbedingungen.

Teil III wird sich als letzter und größter Abschnitt mit dem Verhältnis von Kryptographie und Ethik auseinandersetzen. Zunächst entwickelt Kapitel 5 systematisch-ethische Zugänge zur Kryptographie. Einerseits ist dies der Konsequentialismus und die Pflichtethik, andererseits aber auch ein menschenrechtsbasierter Zugang. Letzterer ist insbesondere vor dem Hintergrund einer *globalen* Kryptographie sinnvoll. Schließlich greift dieser Abschnitt methodologisch nochmals Lessigs Arbeiten auf und unter-

1 Siehe Lawrence Lessig. *Code: Version 2.0*. New York: Basic Books, 2006; sowie Jack Goldsmith und Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. Taschenbuchausgabe. Oxford und New York: Oxford University Press, 2008.

sucht sogenannte *latent ambiguities*. Dies sind unterschwellige Zweideutigkeiten von bestimmten Werten und Normen, die gerade im Bereich der Modernen Kryptographie relevant sein werden.

Anschließend identifiziert Kapitel 6 konsequentialistische Dichotomien im Kontext der Kryptographie, die so (oder so ähnlich) immer wieder im Diskurs genannt werden. Zunächst ist dies die Ansicht, Kryptographie habe einen Dual-Use-Charakter, dann aber auch die Dichotomie, dass Privacy und Sicherheit im Konflikt zueinander stünden, und zuletzt die Vorstellung, dass Kryptographie eine Überwachung unmöglich mache. Alle drei Dichotomien sind auf der Grundlage der Vorarbeiten aus Teil I und Teil II als Schein-Dichotomien zu bewerten, die im Kern nicht der Realität entsprechen.

Daraufhin diskutiert Kapitel 7 drei explizite Spezialthemen der Kryptographie: Transparenz, Gleichheit und Identifikation. Transparenz erscheint zunächst als Gegenentwurf zur Verschlüsselung, insofern das Ziel von Kryptographie unter anderem die Geheimhaltung ist. Tatsächlich aber ist das Verhältnis von Transparenz und Kryptographie mit Blick auf das Whistleblowing komplexer. Im Kontext der Gleichheit soll anschließend eine sogenannte *egalitäre Kryptographie* entwickelt werden. Dies ist eine Kryptographie, die unabhängig von Wissen, Stand, Vermögen und Erfahrung von *jedem* Menschen genutzt werden soll. Und zuletzt ist das Thema der Identifikation zu betrachten, bei dem Kryptographie im Kontext des Schutzzieles der Authentifizierung relevant ist.

Kapitel 8 synthetisiert schließlich die bisherigen Erkenntnisse der Arbeit und wendet sie auf reale, ethisch relevante Problemszenarien an. Zunächst ist das bereits genannte und aktuell relevante *Client-Side-Scanning* (CSS) kritisch zu diskutieren. Anschließend befasst sich das Kapitel mit kryptographischer Regulierung *über Intermediäre*. Dabei wird deutlich, dass eine indirekte Regulierung ethische Probleme aufwirft und im Falle der Kryptographie abgelehnt werden muss. Zuletzt ist nach der Zukunft der (Ethik der) Kryptographie zu fragen. Insbesondere das Quantum Computing wird zeigen, dass eine Ethik der Kryptographie heute relevanter ist denn je.

Mit diesen acht Kapiteln sind die Themen, die die hier vorgelegte Ethik der Kryptographie anreißen wird, umfassend und vielfältig. Bereits an dieser Stelle ist es daher notwendig, bei gewissen Themen eine Abgrenzung vorzunehmen. Denn in allen drei Teilen geht es nicht ausschließlich um Meinungsfreiheit, um Privacy, um Überwachung, um staatliche Eingriffe. Meinungsfreiheit ist zwar im Kontext der Menschenrechte in Ab-

schnitt 5.2 relevant. Privatsphäre ist im Sinne einer Dichotomie von Privacy vs. Sicherheit etwa in Abschnitt 6.2 zu diskutieren. Überwachung ist kritisch in Abschnitt 6.3 zu beleuchten, und Abschnitt 8.2 fragt nach den Eingriffsmöglichkeiten des Staates über Intermediäre. Trotzdem spricht diese Arbeit explizit nicht von einer Ethik *der Meinungsfreiheit*, *der Privatsphäre*, *der Überwachung* oder *der staatlichen Eingriffe*.

Das, was die folgenden Diskussionen vereint, ist der Fokus auf eine Ethik *der Kryptographie*. Denn die Frage, wie wir eigentlich mit Kryptographie umgehen sollen, ist in dieser dedizierten Form bisher nur ungenügend beantwortet worden. Politisch, zivilgesellschaftlich und wirtschaftlich steht Kryptographie zwar immer wieder im Zentrum von argumentativen Auseinandersetzungen. Die Ethik als die Wissenschaft über Moral lässt einen spezifischen, systematischen und umfassenden Zugang zur Kryptographie bislang aber vermissen – trotz der herausragenden Bedeutung der Kryptographie für die moderne Gesellschaft. Die kommenden acht Kapitel werden diese Lücke schließen.

Teil I
Kryptographie & Technologie

Die heute genutzte Kryptographie ist zunächst eine *technologische Angelegenheit*. Auf digitale Weise sicher und vertraulich kommunizieren zu können, erfordert zwangsläufig den Einsatz kryptographischer Algorithmen. Schließlich wollen wir, dass eine digitale Finanztransaktion vertraulich ist und dass sie die gewünschte Person erreicht. Gleichzeitig möchten wir, dass beispielsweise unsere digitalen Gesundheitsdaten sicher verwahrt werden, damit sie nicht von jemand anderem mitgelesen werden können. Und nicht weniger wollen wir, dass niemand unsere intimsten Interessen im Internet erfährt. Eine technologisierte Gesellschaft verlässt sich damit auf die Implementierung von kryptographischen Verfahren.

In einer Zeit, in der Kommunikation noch prä-digital stattfand, war die Bedeutung von Kryptographie nicht vergleichbar mit jener, die sie heute hat. *Bedeutung* meint dabei zunächst gar kein quantifizierbares Kriterium. Es geht viel eher um die Frage, *für wen* Kryptographie Bedeutung hatte und hat. Wir werden in den folgenden Kapiteln sehen, dass in dieser Hinsicht ein fundamentaler Wechsel stattgefunden hat. Noch bis in die Mitte des 20. Jahrhunderts hatte die Kryptographie als Werkzeug des Militärs, der Nationalstaaten, der Diplomatie und der Mächtigen der Welt gegolten.[1] Im Laufe des letzten Jahrhunderts wurde die Kryptographie hingegen für *alle Individuen* von Bedeutung.[2]

Die spezifischen Gründe hierfür werden in den folgenden Abschnitten anhand zweier *Paradigmen* veranschaulicht: einerseits des Paradigmas

1 Menezes, Oorschot und Vanstone erkennen dabei: „The predominant practitioners of the art were those associated with the military, the diplomatic service and government in general. Cryptography was used as a tool to protect national secrets and strategies." Alfred J. Menezes, Paul C. van Oorschot und Scott A. Vanstone. *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1997, S. 1.

2 Siehe Jonathan Katz und Yehuda Lindell. *Introduction to Modern Cryptography*. 2. Aufl. Boca Raton: CRC Press, 2015, S. 1.

der *Klassischen Kryptographie* (Kapitel 1) und andererseits des Paradigmas der *Modernen Kryptographie* (Kapitel 2).[3] Das Konzept des Paradigmas und der damit zusammenhängende *Paradigmenwechsel* (engl. *paradigm shift* oder *paradigm change*) wurden bereits 1962 von Thomas S. Kuhn in seinem einflussreichen Werk *The Structure of Scientific Revolutions* geprägt.[4] Für Kuhn gibt es zwei Charakteristika, durch die eine bestimmte *Leistung* (engl. *achievement*) zum Paradigma wird: Einerseits sei die Leistung „sufficiently unprecedented to attract an enduring group of adherents away from competing modes of scienific activity"[5]. Andererseits sei sie „sufficiently open-ended to leave all sorts of problems for the redefined group of practitioners to resolve"[6].

Sicherlich ist dieser durchaus unscharfe Begriff in den letzten Jahren inflationär verwendet worden. Gleichwohl könnte er für die Entwicklung der Kryptographie passender kaum sein. Was nämlich das 16. Jahrhundert für das astronomische Weltbild bedeutet hatte, war für die Kryptographie das 20. Jahrhundert: eine neue Art und Weise, über Kryptographie als Wissenschaft nachzudenken, um gerade damit sehr erfolgreich spezifische Problemfelder der Praxis zu lösen.[7] Diese neuartige Denkweise und die Bedeutung der Kryptographie sind allerdings nur verständlich mit dem systematischen Wissen um *beide* Paradigmen – das der Klassischen Kryptographie und das der Modernen Kryptographie.

---

3 Die Unterteilung in eine Klassische Kryptographie und eine Moderne Kryptographie findet sich auch in der Literatur; siehe etwa Katz und Lindell, *Introduction to Modern Cryptography* sowie Craig P. Bauer. *Secret History: The Story of Cryptology*. 2. Aufl. Boca Raton, London und New York: CRC Press, 2021.

4 Siehe Thomas S. Kuhn. *The Structure of Scientific Revolutions*. 4. Aufl. Chicago und London: The University of Chicago Press, 2012. Er selbst war gegenüber dem Begriff des Paradigmas später kritisch eingestellt; siehe Ian Hacking. „Introductory Essay". In: Thomas S. Kuhn. *The Structure of Scientific Revolutions*. 4. Aufl. Chicago und London: The University of Chicago Press, 2012, S. vii–xxxvii, hier S. xviii.

5 Kuhn, *The Structure of Scientific Revolutions*, S. 10.

6 Ebd., S. 10–11.

7 Im Paradigma der Klassischen Kryptographie galt kryptographische Forschung als Teil der Linguistik. Sie war, wie der kommende Abschnitt deutlich machen wird, dabei eine zumeist militärische Angelegenheit. Erst mit herausragenden Persönlichkeiten des 20. Jahrhunderts wie dem Mathematiker Claude Shannon wurde Kryptographie im Bereich der Mathematik angesiedelt. Diese neue Art und Weise, über Kryptographie nachzudenken, wurde zum fruchtbaren Boden, auf dem sich das zweite Paradigma der *Modernen Kryptographie* entwickeln konnte. Zu dieser neuen Kryptographie kommen nun Algorithmen und Protokolle hinzu, die über das alleinige Schutzziel von Vertraulichkeit hinausgehen.

Diese modellhafte Systematisierung anhand einer historischen Einteilung ist auch für eine Ethik der Kryptographie erforderlich. Zum einen lassen sich dadurch Begrifflichkeiten klären, die im späteren Verlauf diskutiert werden. Zum anderen hat erst die Entwicklung der Modernen Kryptographie jene fundamentalen, gesellschaftlichen Konflikte hervorgebracht: Wer soll kryptographische Forschung betreiben können? Welche Institution soll Algorithmen standardisieren dürfen? Und überhaupt: Kann Kryptographie für die *good guys* zugänglich gemacht werden – und für die *bad guys* nicht? Für all diese Fragen wird Teil I die technologisch-systematischen Grundlagen liefern.[8]

8 Damit handelt es sich bei Teil I nicht um ein in erster Linie historisches Kapitel, sondern vielmehr um eine technologisch-systematische Einteilung und zugleich Einleitung in die Kryptographie.

1 Klassische Kryptographie

> The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write.
>
> – David Kahn, Autor von *The Codebreakers*[1]

Wenn man bereits mit dem ersten Kapitel in eine wissenschaftliche Auseinandersetzung geraten möchte, dann damit, etwas als *klassisch* zu bezeichnen, sei es in der Musik, Kunst, Mathematik, Politik oder jeglicher anderen Wissenschaft. Für die Kryptographie gilt dies in ähnlicher Weise, denn wer oder was entscheidet schon, was eine klassische Kryptographie sein soll?

Im Kontext dieser Arbeit ist die *Klassische Kryptographie* dialektisch gegenüber einer Art der neuen Kryptographie, der *Modernen Kryptographie*, definiert.[2] Vereinfacht könnte man sagen, dass Klassische Kryptographie in vielerlei Hinsicht das ist, was Moderne Kryptographie nicht ist – und umgekehrt. Diese Dialektik ist zwar nicht willkürlich zu verstehen, doch sagt sie aus: Unsere heutige, Moderne Kryptographie ist nicht verständlich ohne ihren systematisch-historischen Hintergrund. Um diesen Wechsel und seine weitreichenden Auswirkungen auf sowohl die Wissenschaft als auch die Gesellschaft überhaupt nachvollziehen zu können, ist daher das Wissen um das frühere Paradigma notwendig.

Neben diesem dialektischen Ansatz zeichnet sich die Klassische Kryptographie auch dadurch aus, dass sie das beschreibt, was man etymologisch wie auch in der Alltagssprache unter dem Begriff der Kryptographie versteht: Verschlüsselung von Texten, damit Parteien, die die Texte

1 David Kahn. *The Codebreakers: The Story of Secret Writing*. Überarbeitete Version. New York: Scribner, 1996, S. 84; auch zitiert in John F. Dooley. *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*. Cham: Springer, 2018, S. 5.

2 Die Unterscheidung von Klassischer und Moderner Kryptographie wird in der Literatur oft gezogen, so etwa bei Bauer, *Secret History*, sowie Katz und Lindell, *Introduction to Modern Cryptography*. Die zeitlichen und inhaltlichen Grenzen beider Paradigmen unterscheiden sich jedoch teilweise.

nicht lesen *sollen*, sie auch nicht lesen *können*.[3] Für über zweitausend Jahre erfüllte Kryptographie auch just diese Funktion. Erst die Moderne Kryptographie wird diese Definition erweitern.[4] Um sich dieser Klassischen Kryptographie anzunähern, werden im Folgenden zunächst die Anfänge der Kryptographie und Kryptoanalyse beschreiben (Abschnitt 1.1). Anschließend werden mit deren Mechanisierung die ersten Schritte einer Technologisierung der Kryptographie analysiert (Abschnitt 1.2).

1.1 Die Anfänge von Kryptographie und Kryptoanalyse

Mit *The Codebreakers* gelang es David Kahn im Jahr 1967, die grundlegendste und bis dahin aktuellste Geschichte der Kryptographie zu verfassen.[5] Kahn legte damit aber nicht nur ein fundamentales Geschichtsbuch vor, sondern beeinflusste mit seinem Lebenswerk eine ganze Genera-

3 Der Begriff *Kryptographie* ist abgeleitet vom griechischen κρυπτός (dt. *geheim*) und γράφειν (dt. *schreiben*). Damit ist das Schutzziel der Vertraulichkeit gemeint, das sowohl in der Klassischen als auch in der Modernen Kryptographie vorhanden ist.

4 Charakteristisch ist für die Klassische Kryptographie zudem, dass sie manchmal eher als Kunst definiert wird. Siehe zur Diskussion Katz und Lindell, *Introduction to Modern Cryptography*, S. 3. Joachim von zur Gathen charakterisiert die Kryptographie etwa als „the art of making secure systems"; Joachim von zur Gathen. *CryptoSchool*. Berlin und Heidelberg: Springer, 2015, S. 13.

5 Siehe in der Version von 1996 Kahn, *The Codebreakers*. Für Craig Jarvis handelt es sich bei *The Codebreakers* gar um die „authoritative history of cryptology"; Craig Jarvis. *Crypto Wars: The Fight for Privacy in the Digital Age. A Political History of Digital Encryption*. Boca Raton: CRC Press, 2021, S. 71, weiterführend auch 71–74. Neben Kahn werden im Folgenden weitere Geschichtswerke betrachtet, insbesondere Bauer, *Secret History*; Dooley, *History of Cryptography and Cryptanalysis*; sowie Gathen, *CryptoSchool*. Für eine populärwissenschaftliche Einführung siehe auch Simon Singh. *The Code Book: The Secret History of Codes and Codebreaking*. Taschenbuchausgabe. London: Fourth Estate, 2000. Eine konzise Einführung in die Klassische Kryptographie liefert auch Katz und Lindell, *Introduction to Modern Cryptography*, S. 8–16. Historisch wurde im Englischen teilweise zwischen *code* und *cipher* unterschieden, wobei bei Ersterem Wörter des Klartextes mit alphabetischen oder numerischen *codes* ausgetauscht wurden; *cipher* hingegen bezieht sich auf Transformationen von kleineren Elementen des Klartextes. Siehe dazu Whitfield Diffie und Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Überarbeitete und erweiterte Version. Cambridge, MA, und London: MIT Press, 2007, S. 13–14. Im Folgenden wird meist von Verschlüsselung im Sinne der *ciphers* gesprochen.

tion von herausragenden Kryptographinnen und Kryptographen.[6] In der Begründung einer dediziert kryptographischen Geschichtswissenschaft steht *The Codebreakers* metaperspektivisch ganz im Zeichen des Paradigmenwechsels der zweiten Hälfte des 20. Jahrhunderts.[7] Denn seit dessen Veröffentlichung handelt es sich mit jener Forschung zur Geschichte der Kryptographie um ein lebendiges Forschungsfeld. Immer wieder kommen neue, lange Zeit unbekannte Informationen über vergangene kryptographische Methoden ans Licht.[8] Der Zeitpunkt dieser Erkenntnisse ist nun vor allem dadurch bedingt, dass es sich aufgrund des Paradigmenwechsels um ein relativ junges Feld der Geschichtsforschung handelt. Die Kryptographie war über Jahrtausende eine Art Geheimwissenschaft, über deren Fortschritt nur wenig an die Öffentlichkeit oder in Feindeshand gelangen sollte.

Diese längere Zeit der intransparenten und unbekannten Wissenschaft könnte den Eindruck erwecken, dass die Kryptographie selbst eigentlich eine noch sehr junge Disziplin sei.[9] Tatsächlich aber reichen die Ursprünge und die Motivation zum verschlüsselten Kommunizieren historisch weit zurück. David Kahn erkennt sogar eine mögliche Kausalität zwischen dem menschlichen Drang nach Privatsphäre und der Entwicklung der Kryptographie:

---

6 So z. B. Whitfield Diffie; siehe Steven Levy. *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*. New York: Penguin Books, 2002, S. 21–24.

7 Siehe zum Umfeld der 1960er-Jahre und der kryptographischen Geschichtsschreibung auch David Naccache, Peter Y. A. Ryan und Jean-Jacques Quisquater. „Preface". In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Berlin und Heidelberg: Springer, 2016, S. IX–X; sowie Andrew J. Clark. „Foreword". In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Berlin und Heidelberg: Springer, 2016, S. VII–VIII.

8 Vor allem erscheint immer wieder neuere Forschung in der Zeitschrift *Cryptologia*, in der etwa erst 2011 gezeigt wurde, dass das bedeutende *One-Time-Pad* bereits vor Vernam und Mauborgne beschrieben wurde. Siehe Steven M. Bellovin. „Frank Miller: Inventor of the One-Time Pad". In: *Cryptologia* 35.3 (2011), S. 203–222; zu den Hintergründen des Artikels von Bellovin auch Bauer, *Secret History*, S. 102–103.

9 Siehe Charles Berret. „The Cultural Contradictions of Cryptography: A History of Secret Codes in Modern America". Dissertation. New York: Columbia University, 2019. URL: https://academiccommons.columbia.edu/doi/10.7916/d8-3h8z-4t93 (besucht am 15.04.2024), S. 133.

> It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously – as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write. Cultural diffusion seems a less likely explanation for its occurrence in so many areas, many of them distant and isolated.[10]

Solch eine Kryptographie scheint also eng mit zivilisatorischer Entwicklung zusammenzuhängen. Sie ist damit auch immer nicht bloß reine Technologie gewesen, sondern kontextuell eingebunden in politische, soziale, gesellschaftliche und historische Rahmenbedingungen. In ihrer Natur als kommunikatives Werkzeug ist Kryptographie also seit jeher auch eine sozial-gesellschaftliche Sache. Zwar war eine rigorose Verschlüsselung, wie wir sie heute kennen, nicht notwendig, um Informationen geheim zu halten oder verschlüsselt kommunizieren zu können. Lesen und Schreiben war in einer analphabetischen Gesellschaft bereits eine hohe Hürde, sodass weitere Maßnahmen oft nicht erforderlich waren.[11] Manche Texte und Schriften wurden allerdings als eine Art „cosmic top secrets"[12] verstanden und sollten durch weiteren Schutz nur der königlichen Oberschicht zugänglich sein.[13] Nach Kahn begann die (nachgewiesene) Geschichte der Kryptologie vor viertausend Jahren in einem Dorf in der Nähe des Nils:

> On a day nearly 4000 years ago, in a town called Menet Khufu bordering the thin ribbon of the Nile, a master scribe sketched out the hieroglyphs that told the story of his lord's life – and in so doing he opened the recorded history of cryptology.[14]

Natürlich erkennt Kahn auch, dass es sich dabei nicht um ein „system of secret writing"[15] gehandelt hatte, wie es die moderne Welt kenne. Dieser

10 Kahn, *The Codebreakers*, S. 84; zitiert auch in Dooley, *History of Cryptography and Cryptanalysis*, S. 5.

11 Siehe Gathen, *CryptoSchool*, S. 70; sowie Jan Assmann. „Zur Ästhetik des Geheimnisses. Kryptographie als Kalligraphie im alten Ägypten". In: *Zeichen zwischen Klartext und Arabeske. Konferenz des Konstanzer Graduiertenkollegs „Theorie der Literatur". Veranstaltet im Oktober 1992*. Hrsg. von Susi Kotzinger und Gabriele Rippl. Amsterdam und Atlanta: Rodopi, 1994, S. 175–186, hier S. 178.

12 Gathen, *CryptoSchool*, S. 70.

13 Siehe ebd., S. 70; umfassender auch Assmann, „Zur Ästhetik des Geheimnisses".

14 Kahn, *The Codebreakers*, S. 71.

15 Ebd., S. 71.

anonyme Schreiber führte aber zumindest eine absichtliche Transformation des Textes durch.[16] Kahn bezeichnet die Kryptologie des alten Ägyptens daher auch als „quasi cryptology in contrast to the deadly serious science of today“[17].

Auf ähnliche Weise analysiert der Ägyptologe Jan Assmann die Kryptographie als Kalligraphie im alten Ägypten.[18] Schließlich gelang es Jean-François Champollion erst im Jahr 1822, die Bedeutung der Hieroglyphen zu entschlüsseln. Bis zu diesem geschichtlichen Ereignis hatte man sie Assmann zufolge tatsächlich für Kryptographie gehalten. Dies stellte sich als ein „gründliches Mißverständnis“[19] heraus, wie er schreibt – allerdings um ein „interessantes und produktives Mißverständnis“[20]. Bei den Hieroglyphen handelt es sich nämlich keineswegs um irgendeine Form von „Geheimniskrämerei, Verrätselung, Arcanisierung“[21], was aufgrund von Analphabetismus auch nicht notwendig gewesen wäre.[22] Trotzdem gab es nach Assmann verschiedene Formen einer „Kryptographie im literarischen Sinne“[23].

Mit dieser historischen Einordnung dürfte für Teil I deutlich werden: Der konkrete Beginn dessen, was *heute* als Kryptographie verstanden wird, ist teilweise diffus und nur schwer zu lokalisieren. Das Beispiel ägyptischer Hieroglyphen lässt unterschiedliche Ebenen der Beziehung zur Kryptographie zu, die gar bis zu einer „Verrätselung zum Zwecke der Ästhetisierung“[24] reichen konnten. Der Ursprung kryptographischer Kommunikation liegt eben nicht in einer rigorosen Mathematik. Unterschiedliche Ziele, Motive und Methodiken bedeuten ein facettenreiches Bild der Anfänge der Kryptographie.

Bereits an dieser Stelle ist jedoch eine Faszination für die *Verschlüsselung* zu unterscheiden von einer Faszination für das *Verschlüsselte* selbst.

16 Siehe ebd., S. 71.

17 Ebd., S. 72.

18 Siehe dazu und zum Folgenden Assmann, „Zur Ästhetik des Geheimnisses“. Siehe allgemein einführend auch Singh, *The Code Book*, S. 201–217.

19 Assmann, „Zur Ästhetik des Geheimnisses“, S. 175.

20 Ebd., S. 175.

21 Ebd., S. 178.

22 Siehe ebd., S. 178.

23 Ebd., S. 178. So lassen sich Beispiele einer sogenannten *Entkonventionalisierung* finden: „Entweder, die vorhandenen Zeichen erhalten eine andere als die konventionelle Bedeutung, oder es werden andere als die konventionellen Zeichen, d. h. neue Zeichen eingeführt“; ebd., S. 180.

24 Ebd., S. 183.

Erstere ist das, was diese Arbeit als Kryptographie versteht. Letztere dagegen legt den Fokus auf das Verschlüsselte selbst. Dies inkludiert unter anderem die Suche nach Geheimbotschaften, verborgenen Wahrheiten, paranormalen Schriften. Ein prominentes Beispiel ist hierbei die Suche nach solchen versteckten Botschaften, Wahrsagungen und Prophezeiungen in Offenbarungen wie der Bibel.[25] Eine Ethik der Kryptographie, wie sie hier gedacht ist, wird versteckte Prophezeiungen und das Verschlüsselte selbst nicht behandeln. Es geht ihr vielmehr um die Grundlagen von Kryptographie, Technologie und Gesellschaft mit Blick auf die zukünftige Anwendung. Ausschließlich Letzteres ist Untersuchungsgegenstand einer Ethik der Kryptographie.[26]

Eine solche Kryptographie, wie sie im Rahmen dieser Arbeit inkludiert sein könnte, lässt sich aber auch in der hebräischen Bibel finden. Dabei handelt es sich um eine Substitution, die als *atbash*-System bezeichnet wird.[27] Substitutionsmethoden wie im *atbash*-System werden zur sogenannten *symmetrischen* Kryptographie eingesetzt, die für die Zeit der Klassischen Kryptographie charakteristisch ist. *Symmetrisch* meint in diesem Zusammenhang, dass der Schlüssel zum Verschlüsseln (genannt k_e) identisch ist mit dem Schlüssel zum Entschlüsseln (genannt k_d), also $k_e = k_d$.[28] Dies mag auf den ersten Blick sinnvoll oder gar notwendig erscheinen, allerdings wird auch hier der Modernen Kryptographie der

25 Ein Beispiel hierfür ist Drosnins kritisierte Monographie *The Bible Code*. Siehe Michael Drosnin. *The Bible Code*. New York: Simon & Schuster, 1997. Zur berechtigten Kritik an der generell dahinterstehenden Methode der *Equidistant Letter Sequence* siehe Brendan McKay u. a. „Solving the Bible Code Puzzle". In: *Statistical Science* 14.2 (1999), S. 150–173.

26 Noch spezifischer wäre hier das *Verschlüsselte* von der *Methodik* des Verbergens von Nachrichten zu unterscheiden. Bei dieser handelt es sich dann nämlich um eine Form der *Steganographie*. Als Steganographie wird eine Methode bezeichnet, bei der Nachrichten, die geheim gehalten werden sollen, in anderen Nachrichten *verborgen* werden. In gewissem Maße kann die Steganographie als Teil der wissenschaftlichen Kryptographie auch ethisch relevant sein, z. B. im Rahmen des Whistleblowings. Da dies aber eine untergeordnete Rolle spielt, wird es nicht näher diskutiert. Siehe zur Steganographie einführend z. B. Frank Y. Shih. *Digital Watermarking and Steganography: Fundamentals and Techniques*. 2. Aufl. Boca Raton: CRC Press, 2017; sowie Ingemar J. Cox u. a. *Digital Watermarking and Steganography*. Burlington: Morgan Kaufmann, 2008.

27 Siehe Kahn, *The Codebreakers*, S. 77–78; einführend auch Bauer, *Secret History*, S. 19.

28 Üblicherweise werden in der Literatur englische Begriffe verwendet. *k* steht daher für *key*, *e* für *encrypt* und *d* für *decrypt*. Siehe einführend zur symmetrischen Kryptographie z. B. Gathen, *CryptoSchool*, S. 37–38.

Durchbruch gelingen. Einige Forschende werden in den 1970er-Jahren nämlich zeigen, dass k_e nicht zwangsläufig auch k_d sein muss.[29]

Für die symmetrische Kryptographie gibt es zwei grundsätzliche Methodiken zur Ver- und Entschlüsselung: die bereits genannte *Substitution* sowie eine *Transposition*.[30] Bei einer Substitution werden Zeichen eines Alphabets – zum Beispiel Buchstaben – nach einer vorgegebenen Systematik ersetzt. Bei einer Transposition hingegen wird die Anordnung solcher Zeichen vertauscht. Beide Methodiken sind ein wichtiges Bauteil für die symmetrische Verschlüsselung, die in ihrer weiterentwickelten Form bis heute vertrauliche Kommunikation sicherstellen kann.

Die mathematischen Definitionen der beiden Methoden werden an dieser Stelle ausgelassen, jedoch soll die grundsätzliche Idee deutlich gemacht werden: Indem bei einer Transposition (auch Permutation genannt) die *Anordnung* von Zeichen vertauscht wird, könnte beispielsweise aus dem Wort *cryptolove* das Wort *rcpyotolev* werden. Der erste Buchstabe wird dabei mit dem zweiten getauscht, der dritte mit dem vierten usw. Bei der Substitution hingegen werden Zeichen des Klartextes durch Zeichen eines Chiffrentextes *ersetzt*. Mit der Regel, alle *o* durch ein *l* (und umgekehrt) zu ersetzen, würde etwa die Zeichenkette *cryptolove* zu *cryptlolve*. Der womöglich bekannteste Algorithmus einer solchen Substitution ist die sogenannte Caesar-Chiffre.[31] Bei dieser wird jedes Zeichen aus einem geordneten Alphabet des Klartextes zyklisch auf ein Zeichen aus dem geordneten Alphabet des verschlüsselten Textes abgebildet.[32] Mit einem Schlüssel $k = 3$ wird zum Beispiel der Buchstabe a zum Buchstaben d, b zu e, c zu f usw. bis zum Buchstaben z, der zum

29 Die entsprechende Methode wird daher dann auch als *asymmetrische* Kryptographie bezeichnet. Siehe Abschnitt 2.3.

30 Diese heute übliche Teilung wurde bereits im 16. Jahrhundert von Giovanni Battista Porta grob beschrieben; siehe Kahn, *The Codebreakers*, S. 139. Siehe zur folgenden Einführung Katz und Lindell, *Introduction to Modern Cryptography*, S. 10–13; sowie Gathen, *CryptoSchool*, S. 61–69; für den umfassenden historischen Kontext auch Bauer, *Secret History*, S. 3–57 und 107–127.

31 Caesar selbst beschreibt eine Idee der Kryptographie in seinem bekannten Werk *De bello Gallico*. Von der *Caesar-Chiffre* berichtet erstmalig allerdings der römische Geschichtsschreiber Sueton in seinem Werk *De vita Caesarum*. Siehe dazu Kahn, *The Codebreakers*, S. 83–84; sowie Dooley, *History of Cryptography and Cryptanalysis*, S. 13–14. Sie wird häufig in der Didaktik genutzt, um die grundsätzlichen Verfahrensweisen von Kryptographie zu erläutern.

32 Siehe hierzu und zur folgenden Beschreibung einführend Bauer, *Secret History*, S. 7–8. Caesar selbst hatte keine unterschiedlichen Schlüssel verwendet, jedoch ge-

Buchstaben *c* wird. Ein Klartext *cryptolove* wird damit zu *fubswroryh*. Die Entschlüsselung erfolgt anschließend umgekehrt.

Besonders faszinierend ist die Caesar-Chiffre nicht nur aufgrund ihrer Verständlichkeit im pädagogischen Sinne, sondern vor allem durch ihre Historizität. Suetons Beschreibung der Caesar-Chiffre war nach John F. Dooley die erste schriftliche Beschreibung der modernen monoalphabetischen Substitutionsmethode unter Verwendung eines verschobenen Standardalphabets.[33] Bis heute ist das Grundprinzip der Substitution ein entscheidendes Primitiv für praktisch anwendbare Kryptographie. Mit dem Fall des Römischen Reiches verschwand das Wissen über die Kryptographie allerdings für eine gewisse Zeit.[34] Für Dooley wandelte sich die Kryptographie sogar „from a useful technique for keeping communications secret into a dark art that bordered on magic“[35].

Im Mittelalter war es daher auch im arabischen Raum, wo während des islamischen goldenen Zeitalters eine der einflussreichsten Methoden zum Brechen von Substitutionsmethoden entwickelt wurde: die Häufigkeitsanalyse (engl. *Frequency Analysis*), erstmalig beschrieben durch den islamischen Universalgelehrten al-Kindī.[36] Die revolutionäre Erkenntnis dabei war, dass linguistische Charakteristika durch eine monoalphabetische Substitutionsmethode *nicht* versteckt werden. In der englischen Sprache kommt der Buchstabe *e* beispielsweise häufiger vor als *l*, der Buchstabe *k* wiederum häufiger als *x*.[37] Mit einem entsprechend großen Datensatz bestehend aus Briefen, Büchern oder Notizen können die pro-

nügt folgende Beschreibung zur Darstellung der Funktionsweise. Siehe weiterführend Katz und Lindell, *Introduction to Modern Cryptography*, S. 8–10.

33 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 14. Nach Beutelspacher begann die Kryptographie sogar mit Caesar, da dieser einerseits keine Geheimzeichen verwendete und andererseits eine Variabilität eingebaut wurde; siehe Albrecht Beutelspacher. *Geheimsprachen und Kryptographie: Geschichte, Techniken, Anwendungen*. 6. Aufl. München: C. H. Beck, 2022, S. 18–19. Letzterer Aspekt zur Variabilität ist jedoch historisch unklar, da Caesar selbst einen fixen Schlüssel verwendet hatte; siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 8–9.

34 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 15.

35 Ebd., S. 15.

36 Siehe dazu und zur folgenden Beschreibung der Häufigkeitsanalyse ebd., S. 15 und 18. Umfassender zur arabischen Kryptologie auch Gathen, *CryptoSchool*, S. 499–503. Zur Häufigkeitsanalyse siehe einführend Bauer, *Secret History*, S. 17–18.

37 Siehe zur Häufigkeitsverteilung Katz und Lindell, *Introduction to Modern Cryptography*, S. 11.

zentualen Häufigkeiten für alle Buchstaben eines Alphabets einer bestimmten Sprache angegeben werden.

Mit diesem Wissen erfolgt die Entschlüsselung eines mit einer monoalphabetischen Substitutionsmethode verschlüsselten Textes, indem die Vorkommnisse der einzelnen Buchstaben im verschlüsselten Text gezählt werden.[38] In einem längeren verschlüsselten Text fällt dann vielleicht auf, dass der Buchstabe *g* am häufigsten vorkommt. Der Buchstabe *v* am zweithäufigsten usw. Wir wissen zudem bereits, dass das *e* in englischen Klartexten am häufigsten vorkommt, der Buchstabe *t* am zweithäufigsten usw. Uns fällt schließlich auf: Der Buchstabe *g* ist der zweite Buchstabe nach *e*, und auch der Buchstabe *v* ist der zweite Buchstabe nach *t*. Sofern es sich um eine Caesar-Verschlüsselung handelt, können wir daher vermuten, dass der Text mit dem Schlüssel $k = 2$ verschlüsselt wurde.

Diese Häufigkeitsanalyse ist Teil der *Kryptoanalyse*, des Gegenstücks zur Kryptographie. Während die Klassische Kryptographie als die Verschlüsselung von Texten definiert ist, versucht sich die Kryptoanalyse an der Entschlüsselung von bereits verschlüsselten Texten.[39] Die Oberbezeichnung sowohl für die Kryptoanalyse als auch für die Kryptographie ist die sogenannte *Kryptologie*. Heute allerdings wird der Begriff *Kryptographie* in der Praxis oftmals synonym zu Kryptologie verwendet.[40] Ein Grund hierfür liegt sicherlich darin, dass Kryptographie und Kryptoanalyse untrennbar zusammengehören: Ein Algorithmus, der nicht auf mögliche Angriffe per Kryptoanalyse hin untersucht wurde, kann nicht als sicher eingestuft werden. Daher findet bereits seit jeher eine Wechselwirkung von Kryptographie und Kryptoanalyse statt. Es gab Zeiten, in denen Kryptoanalystinnen und Kryptoanalysten im Vorteil waren. Während anderer Zeiten wiederum sollten Kryptographinnen und Kryptographen die

38 Diese und die folgenden Erläuterungen der Entschlüsselung orientieren sich an ebd., S. 11–12. Siehe umfassender auch Gathen, *CryptoSchool*, S. 87–95.

39 Siehe zur Einführung in diese und die folgenden, üblichen Definitionen etwa Bauer, *Secret History*, S. xix–xxi; sowie Kahn, *The Codebreakers*, S. xv–xviii, für die Kryptoanalyse vor allem S. xviii.

40 Martin Hellman sagte einmal in einem späteren Interview bezogen auf die Begriffe *Cryptology* und *Cryptography*: „Yeah. I use the two interchangeably. David Kahn would tell me I'm wrong, and he's probably right, but 'cryptography' has a nicer ring to it than 'cryptology.'" Interview in Hugh Williams. *An Interview with Martin Hellman. Recipient of the 2015 ACM Turing Award*. Palo Alto, 19. Mai 2017. URL: https://amturing.acm.org/pdf/HellmanTuringTranscript.pdf (besucht am 15.04.2024), S. 13.

Oberhand haben – zum Beispiel mit *polyalphabetischen Substitutionsmethoden*, wie wir gleich sehen werden.[41]

Obschon Kryptographie nach David Kahn in der ein oder anderen Form eine zivilisatorisch-kulturelle Folge ist, war die praktische Auseinandersetzung mit ihr doch lange Zeit auch ein gesellschaftliches Nischen- oder Randthema. Wie im Kontext der Anfänge der Kryptographie deutlich geworden ist, galt dies insbesondere für eine Zeit, in der viele Menschen weder schreiben noch lesen konnten. Allein dieses Faktum erlaubte bereits ein gewisses Maß an Vertraulichkeit der verschriftlichten Kommunikation. Erst im Italien der frühen Renaissance lässt sich dann die erste systematische, gut dokumentierte Nutzung im westlichen Europa erkennen.[42] Die Kryptoanalyse, insbesondere die einfache Häufigkeitsanalyse, war zu diesem Zeitpunkt bereits weiterentwickelt und das Reisen war unsicher, sodass briefliche Kommunikation abgefangen werden konnte.[43] Eine solche Situation ist – analogisch gedacht – beim heutigen Internet nicht viel anders: Nachrichten können mitgelesen, mitgeschnitten, abgehört werden. Ähnlich wie zu damaliger Zeit gibt es kaum direkt in den Kommunikationskanälen implementierte Sicherheiten, die die Angriffe verhindern könnten. Kommunikationskanäle mussten damals wie heute als grundsätzlich unsicher gelten.

Besondere Bedeutung hatte in dieser Zeit daher die Entwicklung jener polyalphabetischen Substitutionsmethode durch Leon Battista Alberti, den Kahn als „Father of Western Cryptology"[44] beschreibt. Mit einer monoalphabetischen Substitutionsmethode wie der Caesar-Chiffre wird ein Buchstabe des Alphabets immer durch einen anderen Buchstaben eines Alphabets ersetzt. Da also ein *e* immer durch den gleichen Buchstaben wie etwa *c* substituiert wird, ist der Buchstabe *c* im verschlüsselten Text genauso häufig vorhanden wie der Buchstabe *e* im unverschlüsselten Ursprungstext. Im Gegensatz dazu ist die Idee der polyalphabetischen Substitutionsmethode nun, *mehrere* Alphabete zur Verschlüsselung zu nutzen.[45]

41 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 37.
42 Siehe Gathen, *CryptoSchool*, S. 79.
43 Siehe ebd., S. 79.
44 Kahn, *The Codebreakers*, S. 125, auch S. 130. Siehe zu Alberti einführend auch Gathen, *CryptoSchool*, S. 80–81.
45 Siehe Kahn, *The Codebreakers*, S. 125.

Alberti legte dafür den Grundstein in der zweiten Hälfte des 15. Jahrhunderts.[46] Trithemius entwickelte die *tabula recta*, während Belaso eine Erweiterung des Systems mit einem einfach zu merkenden Schlüsselwort beschrieb, was entschieden zur Sicherheit des Systems beitragen konnte. Giovanni Batista Porta fügte schließlich die Gedanken der drei Gelehrten zusammen. Eine noch sicherere Version polyalphabetischer Kryptographie entwickelte aber Blaise de Vigenère. Seine Idee war dabei die Verwendung eines *autokey*, mit dem die Nachricht selbst als ihr eigener Schlüssel dient. Die Methode allerdings, die später als *Vigenère-Chiffre* bzw. *le chiffre indéchiffrable* (dt. *die nicht entschlüsselbare Verschlüsselung*) bezeichnet wurde und für die Vigenère bekannt geworden ist, ist lediglich eine vereinfachte Version polyalphabetischer Kryptographie.[47]

Eine reine Häufigkeitsanalyse, die bei monoalphabetischen Substitutionsmethoden sehr erfolgreich sein konnte, ist ohne eine Verbesserung selbst bei der vereinfachten Vigenère-Chiffre kaum vielversprechend. Erst im 19. Jahrhundert entwickelten der Mathematikprofessor Charles Babbage sowie der preußische Major Friedrich Wilhelm Kasiski unabhängig voneinander eine Methode, die eine entscheidende Schwäche der Vigenère-Chiffre ausnutzt: Das Schlüsselwort, mit dem das jeweilige Alphabet zur Verschlüsselung gewählt wurde, wiederholt sich in einem längeren Text mehrfach.[48] Identische Teile des Klartextes (z. B. der im Deutschen häufig vorkommende Artikel *der*) können nämlich in einem langen Text mehrfach mit einem gleichen Teil des Schlüssels verschlüsselt worden sein. Mithilfe dieser Erkenntnis wird zunächst die mögliche Schlüssellänge eingegrenzt. Anschließend kann auf jedes einzelne Alphabet wieder eine Häufigkeitsanalyse angewandt werden. Heute bekannt ist diese Methode als *Kasiski-Test*.[49] Trotz der höheren Sicherheit und der revo-

46 Siehe zu Alberti, Trithemius, Belaso, Porta und Vigenère im Folgenden Dooley, *History of Cryptography and Cryptanalysis*, S. 37–39; sowie Bauer, *Secret History*, S. 61–65. Ausführlicher siehe auch Kahn, *The Codebreakers*, S. 125–148. Kahn lehnt dabei auch die Bezeichnung für Trithemius als „Father of Cryptology" ab; siehe ebd., S. 136–137.

47 Siehe dazu im Speziellen Dooley, *History of Cryptography and Cryptanalysis*, S. 39, und Kahn, *The Codebreakers*, S. 148. Eine erste Version eines *autokey* entwickelte Cardano, die allerdings problembehaftet war; siehe ebd., S. 143–144.

48 Siehe hierzu und zur folgenden Beschreibung ebd., S. 204–213, sowie Dooley, *History of Cryptography and Cryptanalysis*, S. 69–71. Für eine eher technische Einführung mit Beispiel siehe Gathen, *CryptoSchool*, S. 241–250.

49 Dabei entdeckte Babbage diese Methode neun Jahre vor Kasiski. Zu den möglichen Gründen für die Benennung sowie als Einführung zu Babbage und Kasiski siehe

lutionären Gedanken blieben polyalphabetische Substitutionsmethoden aber lange Zeit wenig genutzt, zumindest verglichen mit sogenannten *Nomenklaturen*.[50] Einerseits waren polyalphabetische Substitutionsmethoden nämlich langsamer als die Nomenklaturen, andererseits wurde ihrer Genauigkeit nicht wirklich vertraut.[51]

Eine andere Person der Kryptographiegeschichte, die einen vielleicht noch größeren Einfluss auf das Verständnis heutiger Verschlüsselungsmethoden hatte, war aber der Niederländer Auguste Kerkhoffs.[52] Im Jahr 1883 veröffentlicht er sein Werk *La Cryptographie militaire*.[53] Für Kahn ist diese Arbeit neben Portas *De Furtivis Literarum Notis* das zweite großartige „outward-looking"[54] Buch. Er beschreibt es gar als „the most concise book on cryptography ever written"[55]. Das große Problem für die Kryptographie zur damaligen Zeit waren angesichts der Möglichkeit telegraphischer Kommunikation nämlich Anwendungsfragen.[56] Kerckhoffs holte die Kryptographie damit aus ihrem eigenen Dunstkreis heraus und führte sie in ein neues Zeitalter der Kommunikation.

Bedeutend ist dabei vor allem, dass Kerckhoffs die Kryptographie in enger Verbindung mit der Kryptoanalyse dachte.[57] Kryptographie und Kryptoanalyse sind auch in der Modernen Kryptographie keine Gegen-

---

Singh, *The Code Book*, S. 78; außerdem Kahn, *The Codebreakers*, S. 207. Eine weitere, scharfsinnige Methode ist der von William Friedman entwickelte *Index of Coincidence* von 1920. Siehe weiterführend Abschnitt 2.1.

50 Siehe ebd., S. 150–154. Nomenklaturen sind ein System, das einerseits aus Codes und andererseits aus Chiffren besteht. Bestimmte Worte werden bei Nomenklaturen explizit codiert. Siehe zur Definition ebd., S. xvii, sowie Dooley, *History of Cryptography and Cryptanalysis*, S. 10.

51 Siehe Kahn, *The Codebreakers*, S. 150.

52 Sein ursprünglicher und voller Name war etwas länger und zeigt unzweifelhaft seine adelige Herkunft aus einer der ältesten flämischen Familien, nämlich Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhof. Siehe ebd., S. 230.

53 Siehe Auguste Kerckhoffs. „La Cryptographie Militaire: Première partie". In: *Journal des sciences militaires* IX (Jan. 1883), S. 5–38; sowie Auguste Kerckhoffs. „La Cryptographie Militaire: Seconde Partie". In: *Journal des sciences militaires* IX (Feb. 1883), S. 161–191.

54 Kahn, *The Codebreakers*, S. 230.

55 Ebd., S. 233.

56 Siehe ebd., S. 233.

57 Wie Kahn schreibt: „Kerckhoffs established ordeal by cryptanalysis as the only sure trial for military cryptography. It is the judgement which is still used today"; ebd., S. 235. Siehe einführend zu Kerckhoffs auch Bauer, *Secret History*, S. 157–158.

sätze, sondern bedingen einander. Ein kryptographisches System kann nicht als sicher bezeichnet werden, wenn nicht ein möglichst großer Aufwand betrieben wurde und wird, es zu brechen. Wir werden später sehen, wie dies im 20. und 21. Jahrhundert an vielen Algorithmen deutlich wird, zum Beispiel im Rahmen von Standardisierungen von kryptographischen Verfahren wie AES.

Bekannt geworden ist Kerckhoffs aber durch die Beschreibung von sechs Voraussetzungen oder Grundsätzen für ein kryptographisches System.[58] Am wichtigsten für die heutige Kryptographie wurde der zweite Grundsatz, der auch als *Kerckhoffs' Prinzip* bezeichnet wird.[59] Heute sagt dieses Prinzip aus, dass die Sicherheit eines Systems *allein* in der Geheimhaltung des Schlüssels liegen darf.[60] Dieses Prinzip ist damit auch die Antwort auf *Security by Obscurity* – eine Methode, bei der nicht allein der Schlüssel geheim gehalten wird, sondern auch die Funktion und die Verfahrensweise des Systems.[61] Kerckhoffs verband mit seiner Arbeit und diesen Grundsätzen die Kryptographie mit der Telegraphie. Aber auch danach war Kryptographie immer abhängig von den aktuellen technologischen und maschinellen Möglichkeiten, wie der nächste Abschnitt zeigen wird.

58 Diese Grundsätze sind: (1) Das System sollte, wenn auch nicht theoretisch, in der Praxis unknackbar sein. (2) Die Kompromittierung der Details des Systems sollte den Korrespondentinnen und Korrespondenten keine Unannehmlichkeiten bereiten. (3) Der Schlüssel sollte ohne Notizen zu merken und leicht zu ändern sein. (4) Das Kryptogramm sollte sich telegrafisch übertragen lassen. (5) Das Verschlüsselungsgerät sollte tragbar und von einer einzigen Person bedienbar sein. (6) Das System sollte einfach sein und weder die Kenntnis einer langen Liste von Regeln noch geistige Anstrengung voraussetzen. Eigene Übersetzung ausgehend von Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 14, sowie Kahn, *The Codebreakers*, S. 235. Siehe im französischen Original Kerckhoffs, „La Cryptographie Militaire", S. 12.

59 Siehe zu einer aktuelleren und ausführlichen Diskussion zu Kerckhoffs' Prinzip Katz und Lindell, *Introduction to Modern Cryptography*, S. 7–8.

60 Siehe Kahn, *The Codebreakers*, S. 236.

61 Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 8. Manchmal wird die Methode auch als *Security through Obscurity* bezeichnet; siehe Claudia Eckert. *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. 10. Auflage. Berlin und Boston: De Gruyter Oldenbourg, 2018, S. 173.

1.2 Die Mechanisierung der Kryptographie

Der Erste Weltkrieg markiert den letzten größeren militärischen Konflikt, in dem Geheimdienstoffiziere die Ver- und Entschlüsselung *von Hand* verrichten sollten.[62] Bis dahin waren es denn auch meist Einzelne oder kleinere Gruppen, die an der Ver- und Entschlüsselung arbeiteten. Für Whitfield Diffie und Susan Landau war Kryptographie während des Ersten Weltkriegs daher auch mehr „an esoteric than a secret field"[63]. Und für Dooley gibt es zwei Gründe für das Ende einer Vorstellung, die er beschreibt als „romantic notion of the single, driven cryptanalyst working alone through the night to crack the cryptogram that would bring victory to his side"[64].

Der eine Grund sei die Erfindung des Radios und drahtloser Telegraphie.[65] Nicht mehr nur einige wenige Nachrichten konnten pro Tag per Bote oder Telegramm versendet und empfangen werden. Nun war es möglich, ohne größeren Aufwand mithilfe Tausender solcher Nachrichten zu kommunizieren. Dies führte zu der Problematik, dass eine manuelle Ver- und Entschlüsselung dieser unzähligen Nachrichten kaum mehr praktikabel war. Kommunikation wurde omnipräsent – und mit ihr auch die Notwendigkeit einer automatisierten Verschlüsselung dieser Kommunikation.

Der andere Grund für eine Automatisierung liegt Dooley zufolge in der Idee, Ver- und Entschlüsselung durch Maschinen zu ermöglichen.[66] Während Substitution, Codebücher, Permutationsalgorithmen und Schlüsseladditionen seit bereits mehreren hundert Jahren Verwendung gefunden hatten, blieb die breite Anwendung von Kryptographie mithilfe von elektromechanischen Maschinen und später auch Computern dem 20. Jahrhundert vorbehalten.[67] Für die Patentierung und den

62 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 87. Zur kryptographischen Geschichte des Ersten Weltkriegs siehe Bauer, *Secret History*, S. 163–198; sowie John F. Dooley. *Codes, Ciphers and Spies: Tales of Military Intelligence in World War I*. Cham: Copernicus, 2016.

63 Diffie und Landau, *Privacy on the Line*, S. 58.

64 Dooley, *History of Cryptography and Cryptanalysis*, S. 87.

65 Siehe dazu und zu diesem Absatz ebd., S. 87.

66 Siehe ebd., S. 88.

67 Siehe für eine visuelle Darstellung dieser verhältnismäßig doch kurzen Episode der elektromechanischen Maschinen seit dem 20. Jahrhundert Gathen, *CryptoSchool*, S. 70.

Verkauf solcher Maschinen wurde vor allem die Zeit zwischen den beiden Weltkriegen genutzt.[68]

Man könnte daher auch von einer *Mechanisierung der Kryptographie* sprechen, die zur entscheidenden Bedingung für den späteren Erfolg von Verschlüsselungstechnologie werden sollte.[69] Zwar gab es bereits weitaus früher Ideen, Ver- und Entschlüsselung zu mechanisieren, beispielsweise bei Alberti, Jefferson und Leibniz.[70] Allerdings ermöglichte erst die erste Hälfte des 20. Jahrhunderts die praktische und weitverbreitete Anwendung solcher kryptographischen Maschinen. Die heute bekannteste Maschine dieser Art war *Enigma*, die vorwiegend im Zweiten Weltkrieg genutzt wurde und deren Bezeichnung an das griechische Wort αἴνιγμα (dt. *Rätsel*) angelehnt ist.[71]

Dabei handelt es sich um eine elektromagnetische Chiffriermaschine, die eine Menge an Polyalphabeten zur Ver- und Entschlüsselung erzeugt, wobei dieselbe Einrichtung und Prozedur sowohl für die Ver- als auch für die Entschlüsselung verwendet wird.[72] Entwickelt wurde diese Maschine ursprünglich vom deutschen Unternehmer Arthur Scherbius. Später wurde Enigma über den gesamten Kriegsverlauf von Deutschland als ausgereifte Verschlüsselungsmethode zur militärischen Kommunikation genutzt und dabei immer wieder verbessert. Aber trotz der ausgefeilten Mechanik war es möglich, Enigma zu brechen. In den 1970er-Jahren erfuhr man von der laut David Kahn „greatest codebreaking operation of the Second World War“[73], genannt *Ultra*, die in Bletchley Park (UK)

68 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 88.

69 Auch Diffie und Landau sowie Singh sprechen von einer *Mechanisierung*; siehe Diffie und Landau, *Privacy on the Line*, S. 57–60, und Singh, *The Code Book*, S. 101–142.

70 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 137. Zu Leibniz siehe Nikolas Rescher. „Leibniz's Machina Deciphratoria: A Seventeenth-Century Proto-Enigma“. In: *Cryptologia* 38.2 (2014), S. 103–115.

71 Siehe einführend zu Enigma Bauer, *Secret History*, S. 217–260.

72 Siehe dazu und zur folgenden Beschreibung von Enigma Dooley, *History of Cryptography and Cryptanalysis*, S. 142 und 151–153; sowie Gathen, *CryptoSchool*, S. 719–725. Die Maschine verwendete unter anderem mehrere *Rotoren*, eine sogenannte *Umkehrwalze*, in manchen Versionen ein *Steckerbrett* sowie die Möglichkeit, die Anordnung der Rotoren zu tauschen; als Schlüssel sind ein *Day Key* und ein *Message Key* erforderlich. Siehe zur Einführung in die Funktionsweise Singh, *The Code Book*, S. 127–142, sowie Bauer, *Secret History*, S. 220–224.

73 Kahn, *The Codebreakers*, S. 972, weiterführend S. 972–978; ausführlicher David Kahn. *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943*. Überarbeitete Auflage. London: Frontline Books, 2012.

durchgeführt worden war. Maßgeblich beteiligt am Erfolg dieser Operation war der Mathematiker Alan Turing, der aufgrund seiner theoretischen Überlegungen als Pionier der Informatik und der Entwicklung des Computers gilt.[74] Turing und sein Team konnten in Bletchley Park auf polnische Vorarbeiten zurückgreifen, die kurz vor Beginn des Zweiten Weltkriegs mit den Alliierten geteilt worden waren.[75] Nach Dooley handelte es sich bei den polnischen Arbeiten gar um „the first analytical break of a cipher machine by mathematicians turned cryptanalysts".[76] Mit der Kryptoanalyse von Enigma sollte die Mathematik sich also als Wissenschaft der Kryptoanalyse bewähren – ein Vorgeschmack auf das Zeitalter Moderner Kryptographie.

Mit den Modifikationen, die Deutschland nach den kryptoanalytischen Erfolgen Polens eingeführt hatte, waren jedoch die rein mathematischen Methoden nicht mehr zielführend.[77] Zu viele Möglichkeiten von Polyalphabeten machten einen neuen Ansatz erforderlich, der an die *Mechanisierung der Kryptographie* auch im Rahmen der Kryptoanalyse anknüpfen sollte. Die Idee, die Alan Turing verfolgte, war eine sogenannte *Probable-Word*-Attacke, die darauf abzielt, wahrscheinliche Wörter im verschlüsselten Text zu identifizieren.[78] Dazu entwickelte er eine Maschine, genannt *bombe*.[79] Diese Maschine reduzierte die Anzahl von möglichen Schlüsseln, die anschließend von Hand getestet werden mussten. Dadurch war es den Alliierten im Verlauf des Zweiten Weltkriegs immer wieder möglich, mit Enigma verschlüsselte Nachrichten zu entschlüsseln. Zu Kriegsende vermochten sie sogar Nachrichten einer noch weiter verbesserten Version von Enigma zu dechiffrieren.

74 Breitere Bekanntheit erlangte Turing auch durch den sogenannten *Turing-Test*; siehe Alan M. Turing. „I.—Computing Machinery and Intelligence". In: *Mind* LIX.236 (1950), S. 433–460.

75 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 156. Zur Einführung in das Brechen von Enigma siehe Singh, *The Code Book*, S. 143–189. Tatsächlich war es den Kryptoanalysten Marian Rejewski, Henryk Zygalski und Jerzy Rozycki gelungen, eine frühere Version von Enigma mit mathematischen Methoden zu brechen. Siehe ausführlicher Bauer, *Secret History*, S. 226–242.

76 Dooley, *History of Cryptography and Cryptanalysis*, S. 151.

77 Siehe ebd., S. 156.

78 Siehe ebd., S. 156. Die *Probable-Word*-Attacke hatte bereits Porta beschrieben. Wenn das Thema des Textes bekannt war, konnten wahrscheinlich vorkommende Wörter ausprobiert werden. Siehe Kahn, *The Codebreakers*, S. 140.

79 Siehe dazu und zur folgenden Beschreibung des Erfolgs gegen Enigma während des Zweiten Weltkriegs Dooley, *History of Cryptography and Cryptanalysis*, S. 157.

Die Bedeutung von Bletchley Park und Enigma lässt sich an der späteren historiographischen Rezeption verdeutlichen. Simon Singh schreibt beispielsweise, dass wohl „[e]inige, wenn auch umstrittene Stimmen behaupteten, die Leistungen von Bletchley Park seien entscheidend für den Sieg der Alliierten gewesen“[80]. Für Kahn half das Wirken in Bletchley Park zumindest die Atlantikschlacht zu gewinnen, jedoch gilt für ihn die Entschlüsselung nicht als allein entscheidend für den Sieg.[81] Er hinterfragt dabei auch zu Recht die grundsätzliche Quantifizierbarkeit des Einflusses dieses Ereignisses. Für Singh ist hingegen sicher, dass das Wirken in Bletchley Park den Krieg wesentlich verkürzt und viele weitere Opfer verhindert hat.[82]

Diese beispielhafte Episode zeigt für die Relevanz einer Ethik der Kryptographie, dass die Kryptographie im letzten Jahrhundert zunehmend Einfluss auf die sozial-gesellschaftliche Umgebung haben konnte. Die Wissenschaft der Verschlüsselung war immer auch eingebunden in komplexe Zusammenhänge aus Wirtschaft, Politik und Militär. Zum einen entwickelte sich über die Jahrhunderte ein Wechselspiel von denen, die Verschlüsselungsmethoden entwickelten, und jenen, die diese Methoden brechen wollten. Die Partei, die dann selbst vertraulich kommunizieren konnte und gleichzeitig die Nachrichten der anderen Partei zu entschlüsseln vermochte, war im entscheidenden Vorteil.

Zum anderen zeigt dieser historische Abriss der Klassischen Kryptographie, dass Verschlüsselung auch stets von den jeweils möglichen

80 Simon Singh. *Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets*. 17. Aufl. München: dtv, 2022, S. 230. Siehe außerdem auch Beutelspacher, *Geheimsprachen und Kryptographie*, S. 33. Zur Rezeption siehe zudem Bauer, *Secret History*, S. 253–254.

81 Siehe dazu und zur folgenden Kritik an der Quantifizierbarkeit David Kahn. „The Significance of Codebreaking and Intelligence in Allied Strategy and Tactics“. In: *Cryptologia* 1.3 (1977), S. 209–222, vor allem S. 218–219; sowie Kahn, *The Codebreakers*, S. 978.

82 Siehe Singh, *Geheime Botschaften*, S. 230. Auch in der Medienkultur wurde das Ereignis im Film *The Imitation Game* mit Benedict Cumberbatch als Alan Turing rezipiert, wenn auch historisch teilweise fragwürdig. Chris Christensen kam in seiner Kritik – erschienen in der kryptographisch-historischen Fachzeitschrift *Cryptologia* – zu dem Schluss, dass die künstlerische Freiheit mit Blick auf die historischen Ereignisse doch zu weit gegangen sei; siehe Chris Christensen. „Review of *The Imitation Game*“. In: *Cryptologia* 41.2 (2017), S. 178–181. Der Film war inspiriert durch Andrew Hodges' Biographie über Alan Turing; siehe Andrew Hodges. *Alan Turing: The Enigma*. Princeton und Oxford: Princeton University Press, 2014.

Kommunikationskanälen und Technologien abhing. In einer Zeit, in der die Bevölkerung zum größten Teil weder lesen noch schreiben konnte, war Kryptographie zur Geheimhaltung von verschriftlichter Information kaum notwendig. Mit der Kommunikationsflut infolge der Telegraphie allerdings wurde Information ubiquitär. Keine Partei konnte mehr auf Kryptographie verzichten. Die Methodiken der Verschlüsselung mussten sich daher an die neuen Realitäten der Technologie anpassen. Kerckhoffs und die Mechanisierung der Kryptographie waren darauf die Antwort.

Enigma steht aber auch sinnbildhaft für eines der letzten Großereignisse vor dem Übergang der Klassischen Kryptographie in ein neues Paradigma. Dieses neue Paradigma sollte nämlich erstmals überhaupt eine fundamentale und dezidierte Beschäftigung der Ethik mit Kryptographie notwendig machen. Bis einschließlich der 1940er- und 1950er-Jahre war die Entwicklung der Kryptographie normativ betrachtet schließlich eher eine *dunkle* Geschichte, die dem einzelnen, gewöhnlichen Individuum wenig bis keinen Vorteil zu bringen vermochte. Kryptographie wurde genutzt zur Kriegsführung, zu einer Art Geheimniskrämerei, zum Schutz vor Informationsverbreitung.[83]

Kryptographie war bis dahin also ein geheimnisvolles Mittel der Mächtigen – und *nur* der Mächtigen. Wer mächtig war, konnte Kryptographie nutzen. Und wer Kryptographie nutzte, wurde noch mächtiger. Im kommenden Paradigma der Modernen Kryptographie hingegen muss niemand schon zuvor in irgendeiner Form mächtig, wohlhabend oder einflussreich sein, um Kryptographie nutzen zu können. Kryptographie sollte nun keine Kunst mehr sein, die einige wenige in den Kammern der Herrschenden durchdenken, entwickeln, brechen und einsetzen. Denn die unzensierte Mathematik wird zur Wissenschaft der Kryptographie. Und genauso wie menschliche Kommunikation wird Kryptographie ubiquitär.

83 Andrew J. Clark erkennt daher in seinem Vorwort zur Festschrift zu Kahns 85. Geburtstag auch: „From its first routine adoption by the Spartans in the fifth century BC, cryptography has been the domain of the military, governments, and spies. Governments throughout the ages have strived to control the dissemination of information relating to cryptology […] and its widespread usage." Clark, „Foreword", S. VII.

2 Moderne Kryptographie

> The universe believes in encryption.
> – Julian Assange, Gründer von *Wikileaks*[1]

In der Klassischen Kryptographie war die Anwendung verschlüsselter Kommunikation in weiten Teilen nur jenen möglich, die Wissen, Macht, Fähigkeiten und die Technik dazu hatten.[2] Die zweite Hälfte des 20. Jahrhunderts markiert jedoch den Anfang des Paradigmas der *Modernen Kryptographie*. Die Entwicklung hin zu dieser neuen Art der Kryptographie fassen Katz und Lindell wie folgt zusammen:

> [C]ryptography has gone from a heuristic set of tools concerned with ensuring secret communication for the military to a science that helps secure systems for ordinary people all across the globe.[3]

Adams erkennt mit Blick auf Katz und Lindell drei entscheidende Neuerungen: (1) Kryptographie als Wissenschaft, (2) die die Sicherheit der Systeme zum Ziel hat und (3) die dies für gewöhnliche Menschen überall auf der Erde ermöglicht.[4] Rigorose Wissenschaft wurde die Kryptographie vor allem durch den Mathematiker Claude Shannon, der dafür die theoretischen Grundlagen lieferte (Abschnitt 2.1). Aber auch die Entwicklungen der kryptographischen Standards (Abschnitt 2.2) und die asymmetrische Kryptographie (Abschnitt 2.3) sind Ausdruck dieses wissenschaftlichen

1 Julian Assange u. a. *Cypherpunks: Freedom and the Future of the Internet*. New York und London: OR Books, 2012, S. 4.

2 Nach Dooley also „an arcane science, known only to a few and jealously guarded by governments, exiled kings and queens, and religious orders." Dooley, *History of Cryptography and Cryptanalysis*, S. vii.

3 Katz und Lindell, *Introduction to Modern Cryptography*, S. 3; auch zitiert in Carlisle Adams. *Introduction to Privacy Enhancing Technologies: A Classification-Based Approach to Understanding PETs*. Cham: Springer, 2021, S. 242. Für Katz und Lindell zeichnet sich die Moderne Kryptographie auch durch eine zentrale Rolle von Definitionen, die Wichtigkeit von formalen und präzisen Annahmen sowie die Möglichkeit rigoroser Beweise von Security aus. Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. xv–xvi sowie 16–23.

4 Siehe Adams, *Introduction to Privacy Enhancing Technologies*, S. 242.

Charakters. Insofern Kryptographie nun außerdem mehr als nur Vertraulichkeit der Kommunikation zum Ziel hatte, wurde sie zu einem bedeutenden Teil ganzheitlicher Informationssicherheit (Abschnitt 2.4). In all diesen Kontexten relevant ist heute auch das Verhältnis von Quantum Computing und Verschlüsselung (Abschnitt 2.5).

Die Folge dieses wissenschaftlichen Fokus auf die digitale Sicherheit ist der ubiquitäre und globale Anspruch einer Modernen Kryptographie. Eine Kryptographie nämlich, die nicht ubiquitär wäre, würde eine Asymmetrie von Staat und Individuum schaffen. Und eine Kryptographie, die nicht global wäre, wäre nicht auf diese Weise im weltweiten Internet nutzbar. Mit der Modernen Kryptographie findet Verschlüsselung heute also Anwendung im World Wide Web, im Online-Banking, in der Telefonie, in Smartcards und vielem mehr. Die allermeisten Menschen sind bewusst oder unbewusst auf Verschlüsselungstechnologien angewiesen. Mit dieser Ubiquität könnte man auch sagen: Die Gesellschaft des 21. Jahrhunderts erlebt – tagtäglich und global – die Auswirkungen dieses Paradigmenwechsels.

Dieser Paradigmenwechsel zeigt einerseits die Notwendigkeit und Relevanz einer *Ethik der Kryptographie*. Ohne eine weitverbreitete und ubiquitäre Kryptographie wäre ein solches soziales, politisches und ökonomisches Leben, wie wir es heute kennen, im digitalen Zeitalter kaum möglich. Zugleich beschreibt dieser Paradigmenwechsel aber auch grundlegende strukturelle Veränderungen einer Gesellschaft, in der Kryptographie eben *in der Mitte* der Gesellschaft angekommen ist – und nicht mehr nur der Diplomatie, dem Militär oder Geheimdiensten zur Verfügung stehen sollte. Erst mit einem Wissen um diese fundamentalen Entwicklungen im 20. Jahrhundert wird die Relevanz der Beziehung von Staat und privater Kommunikation, von Cypherpunks und Crypto-Anarchie, von einer Unterdrückung der Verschlüsselung und dem Verhältnis von Internet, Kryptographie und Regulierbarkeit verständlich.

2.1 Ein neues Paradigma durch die Mathematik

Neben jener *Mechanisierung* von Verschlüsselung, wie sie das letzte Kapitel diskutiert hat, liegt der Modernen Kryptographie vor allem ein Wechsel der Disziplin zugrunde: Bis zum Beginn des 20. Jahrhunderts war die Kryptographie insbesondere Teil der *Linguistik*, die zumeist von einigen wenigen händisch durchgeführt wurde. In der Praxis basierten beispiels-

weise die Caesar-Verschlüsselung und die Vigenère-Chiffre auf einem natürlichsprachlichen Alphabet.

Mit veränderten Kommunikationsformen wie der Telegraphie und später dem Internet musste Kryptographie aber nicht nur sicher und vertraulich sein, sondern eben auch praktikabel und performant: Die Mathematik begann, die Linguistik als Disziplin der Kryptographie abzulösen. Nach Katz und Lindell verfolgt die Moderne Kryptographie im Unterschied zur Klassischen Kryptographie nämlich keinen Ad-hoc- oder informellen Ansatz mehr – sie hat nun vielmehr einen *rigorosen* Anspruch.[5] Dieser zeichnet sich aus durch eine zentrale Rolle von Definitionen, die Wichtigkeit von formalen und präzisen Annahmen sowie die Möglichkeit rigoroser Beweise von Sicherheit.[6] Es steht daher weniger die (oftmals durchaus systematische) Knobelei im Zentrum kryptographischer Ver- und Entschlüsselung, sondern die Rigorosität von mathematischer Beweisführung und Orientierung an logischen und probabilistischen Prinzipien.

Auch Diffie und Helmann schreiben 1976 in ihrem einflussreichen Artikel *New Directions in Cryptography*, dass erst die theoretischen Entwicklungen in der Informationstheorie und Informatik beweisbar sichere kryptographische Systeme ermöglicht hatten.[7] Erst dadurch hätte sich „this ancient art into a science"[8] gewandelt.[9] Und für Dooley basiert die Moderne Kryptologie auf den Arbeiten von drei Männern mit seltenem Talent, die die Kryptologie „from an esoteric, mystical, strictly linguistic

5 Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. xv und 22.

6 Siehe ebd., S. xv–xvi und 16–23.

7 Siehe Whitfield Diffie und Martin E. Hellman. „New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), S. 644–654, hier S. 644.

8 Ebd., S. 644.

9 Im Folgenden soll deutlich werden, dass es tatsächlich Claude Shannon und die von ihm entwickelte Informationstheorie waren, die die späteren Kryptographinnen und Kryptographen beeinflusst hatten. Neben Diffie beeinflusste Shannon z. B. auch Horst Feistel, den Entwickler des einflussreichen symmetrischen Kryptosystems *Lucifer*; siehe Levy, *Crypto*, S. 44–45. Für Katz und Lindell ist die *Moderne* Kryptographie jene Kryptographie, die nach den 1980er-Jahren existiert; siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. xv. Abgeschlossen war der Paradigmenwechsel sicherlich erst in den 1980er-Jahren – begonnen hatte das neue Paradigma mit Blick auf Shannon allerdings bereits einige Jahrzehnte zuvor.

realm into the world of mathematics and statistics“[10] bewegten: William F. Friedman, Lester S. Hill und Claude E. Shannon.[11]

Willian F. Friedman entwickelte mit seiner bekanntesten Schrift *The Index of Coincidence and Its Application to Cryptography* aus dem Jahr 1920 eine Möglichkeit, die Länge des Schlüssels bei einer polyalphabetischen Substitutionsmethode zu schätzen.[12] Zwar hatten bereits zuvor Babbage und Kasiski Methoden beschrieben, wie eine Vigenère-Chiffre gebrochen werden kann. Das Besondere an Friedmans Methode war allerdings, dass sie noch weitaus mehr auf den Grundlagen einer rigorosen Statistik fußte. Um es mit den Worten Kahns auszudrücken: „Friedman led cryptology out of this lonely wilderness and into the broad rich domain of statistics. He connected cryptology to mathematics.“[13]

Lester S. Hill verband wenige Jahre später Kryptographie und Algebra mit seinem Artikel *Cryptography in an Algebraic Alphabet*.[14] Diese Publikation war die erste einer solchen Art, die die abstrakte Algebra mit Kryptographie verknüpfte.[15] Dabei entwickelte er ein neues System polygraphischer Ver- und Entschlüsselung – später als *Hill Cipher* bezeichnet –, das auf invertierbaren quadratischen Matrizen als Schlüsselelement basiert.[16] Der praktische Nutzen dieser Methode war zwar eher gering, allerdings verstärkte Hill den neuen Einfluss der Mathematik auf die Kryptographie.[17]

Die größte Bedeutung für die Moderne Kryptographie dürfte aber zweifelsfrei jener schüchterne, aber doch vielseitig interessierte US-Ame-

10 Dooley, *History of Cryptography and Cryptanalysis*, S. 167.

11 Siehe ebd., S. 167.

12 Siehe Bauer, *Secret History*, S. 66–75, sowie Dooley, *History of Cryptography and Cryptanalysis*, S. 124. Siehe im Original William F. Friedman. *The Index of Coincidence and Its Application to Cryptography*. Riverbank Publications 22. Paris: L. Fournier, 1922.

13 Kahn, *The Codebreakers*, S. 383–384; auch zitiert in Dooley, *History of Cryptography and Cryptanalysis*, S. 125.

14 Siehe Lester S. Hill. „Cryptography in an Algebraic Alphabet“. In: *The American Mathematical Monthly* 36.6 (1929), S. 306–312. Zur Einführung Kahn, *The Codebreakers*, S. 404–410. Gewöhnlicherweise wird die sogenannte Matrixverschlüsselung Hill zugeschrieben. Tatsächlich allerdings war ihm aus historischer Sicht Levine in weiten Teilen zuvorgekommen. Siehe zu den Hintergründen Bauer, *Secret History*, S. 199–201.

15 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 167.

16 Siehe ebd., S. 167.

17 Siehe ausführlicher Kahn, *The Codebreakers*, S. 408–410.

rikaner gehabt haben: Claude Elwood Shannon.[18] Zunächst begründete Shannon mit der Arbeit *A Mathematical Theory of Communication* im Jahr 1948 die Informationstheorie.[19] Ein Jahr später veröffentlichte er sein zweites wichtiges Werk: *Communication Theory of Secrecy Systems*.[20] Dabei formulierte er die formalen und sprachlichen Grundlagen für die heutige Kryptographie. Zahlreiche Begriffe, die bis heute standardmäßig die Sprache der Modernen Kryptographie prägen, wurden durch Shannon definiert.[21] Für Dooley vollendete Shannon daher, was Friedman begonnen und Hill fortgeführt hatte.[22]

Shannons theoretische Brillanz lässt sich beispielhaft an seiner Analyse des *One-Time-Pad* (OTP) zeigen, das bereits einige Jahrzehnte zuvor entwickelt worden war.[23] Das OTP funktioniert wie folgt: Wenn wir einen Klartext (in Bits) in einen verschlüsselten Text (in Bits) chiffrieren wollen, benötigen wir einen zufälligen Schlüssel (in Bits).[24] Dieser muss die gleiche Länge haben wie die zu verschlüsselnde Nachricht. Dann wird eine XOR-Operation mit dem ersten Bit des Klartextes und dem ersten Bit des Schlüssels durchgeführt, anschließend für das zweite Bit, das dritte Bit usw. Das Ergebnis dieser Operationen ist schließlich der verschlüs-

18 Interessiert war er beispielsweise an Schach, Jazz oder Science-Fiction, wobei diese Hobbys wohl durchaus oft wechseln konnten. Siehe ebd., S. 744; teilweise auch genannt in Levy, *Crypto*, S. 17–18, der hier allerdings keine direkte Quellenangabe aufführt. Zur kurzen Biographie von Shannon siehe Ioan James. „Obituary: Claude Elwood Shannon 1916–2001". In: *Bulletin of the London Mathematical Society* 46.2 (2014), S. 435–440; umfassender auch Bauer, *Secret History*, S. 327–343.

19 Siehe Claude E. Shannon. „A Mathematical Theory of Communication". In: *The Bell System Technical Journal* 27.3 (1948), S. 379–423.

20 Siehe Claude E. Shannon. „Communication Theory of Secrecy Systems". In: *The Bell System Technical Journal* 28.4 (1949), S. 656–715.

21 Beispiele wären *diffusion*, *confusion* oder *redundancy*. Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 168.

22 Siehe ebd., S. 168.

23 Eine Einführung zum OTP findet sich etwa bei Gathen, *CryptoSchool*, S. 375–377, sowie im historischen Kontext bei Bauer, *Secret History*, S. 92–96. Gewöhnlich wird Gilbert S. Vernam Anerkennung für diese Entdeckung während des Ersten Weltkrieges gezollt. Tatsächlich allerdings hatte der Bankier Frank Miller ein solches System bereits 35 Jahre zuvor beschrieben, wie Bellovin zeigen konnte. Siehe dazu Bellovin, „Frank Miller". Nach Bellovin ist es allerdings unklar, wem Anerkennung „with *effectively* inventing the one-time pad" zugesprochen werden sollte; ebd., S. 204, kursiv im Original. Bauer berichtet über die Hintergründe dieses Artikels; siehe Bauer, *Secret History*, S. 102–103.

24 Siehe dazu und zur folgenden Beschreibung beispielsweise Gathen, *CryptoSchool*, S. 375–377.

selte Text. Der Schlüssel wird, da es sich um ein symmetrisches Protokoll handelt, sowohl zur Ver- als auch zur Entschlüsselung verwendet.

Das Besondere an diesem Algorithmus ist nun, dass Shannon beweisen konnte, dass das One-Time-Pad tatsächlich *perfect secrecy* ermöglicht.[25] Vereinfacht ausgedrückt meint dies, dass eine Kenntnis des verschlüsselten Textes *keine* Information über den Klartext liefert. Wenn böswillige Angreifende den verschlüsselten Text erhalten, gibt es für sie ohne den Schlüssel keine Möglichkeit, an Informationen des Klartextes zu gelangen, denn der verschlüsselte Text enthält schlicht keine Information über den Klartext. Für das OTP gilt daher auch die Eigenschaft, dass ein böswilliger Akteur oder eine böswillige Akteurin auch mit unbegrenzter Rechenkapazität die Nachricht nicht entschlüsseln könnte. Damit ist das OTP also *information-theoretic secure*. Sind kryptographische Verfahren hingegen lediglich *computationally secure*, dann bedeutet dies, dass bei jedem Angriff eine winzige Chance des Erfolgs besteht.

Warum aber wird dann das OTP nicht öfter eingesetzt, zum Beispiel in der täglichen Internetkommunikation? *Perfect secrecy* respektive *information-theoretic security* erreicht das OTP nur, wenn einige entscheidende Eigenschaften erfüllt sind.[26] Erstens muss der Schlüssel des OTP wie bereits erwähnt so lang sein wie die Nachricht selbst. Zweitens muss er tatsächlich *zufällig* sein. Und drittens darf er auch nur einmal verwendet werden.[27] Diese Bedingungen sind oftmals nur schwer zu erreichen oder zumindest wenig praktikabel. In der Praxis handelt es sich also stets um einen Trade-off von Schnelligkeit, Praktikabilität und Sicherheit. Wenn gewisse Informationen strikt geheim gehalten werden mussten, dann wurde das OTP historisch in sehr spezifischen Fällen allerdings bereits angewandt.[28]

---

25 Siehe dazu und zu diesem Absatz die Beschreibung bei Katz und Lindell, *Introduction to Modern Cryptography*, S. 29, 32–34 und 43; ebenso Dietmar Wätjen. *Kryptographie: Grundlagen, Algorithmen, Protokolle.* Wiesbaden: Springer Vieweg, 2018, S. 4–11.

26 Siehe dazu und zu den bekannten Eigenschaften beispielsweise Paul C. van Oorschot. *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin*. Cham: Springer, 2021, S. 32–33.

27 Beispielsweise verwendete die Sowjetunion Schlüssel mehrmals, wodurch die USA Nachrichten im Rahmen des *Venona-Projekts* entschlüsseln konnten. Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 34.

28 Beispielsweise war die Kommunikationsverbindung des US-amerikanischen Präsidenten zum russischen Präsidenten (auch der *heiße Draht* genannt) über ein OTP verschlüsselt. Siehe Singh, *The Code Book*, S. 124. Allgemeiner zu den Einsatzmög-

Die meisten Algorithmen, die in den folgenden Abschnitten besprochen werden und die in der Praxis üblich sind, erfüllen daher das Kriterium einer *perfect secrecy* nicht und sind lediglich *computationally secure*. Sie gelten trotzdem praktisch betrachtet als sicher, weil ein Angriff mit den heute verfügbaren Rechenressourcen mehrere Jahrmillionen oder mehr zur Entschlüsselung dauern würde. Prinzipiell allerdings gilt für diese Algorithmen, dass der verschlüsselte Text Informationen über den Klartext enthält. Dies ist allein schon dadurch der Fall, dass der Schlüssel bei diesen Algorithmen kürzer ist als der zu verschlüsselnde Text.[29]

Ungeachtet dieser Einschränkungen lässt sich mit Shannon der Beginn eines neuen Paradigmas der Kryptographie verorten – vor allem aufgrund der qualitativen Neuausrichtung an rigoroser Mathematik, Statistik und Informationstheorie, ohne die die Moderne Kryptographie nicht in der heutigen Form existieren würde. Shannons Werk wurde damit zur notwendigen Bedingung für die Moderne Kryptographie. Für Gesellschaft und Ethik ist aber auch wichtig: Wir sehen den Anfang eines grundlegenden Wechsels hinsichtlich der Autorität, die über die Kryptographie bestimmt. Seit 2500 Jahren war kryptographisches Denken – manchmal mehr, manchmal weniger – eine wenig transparente Arbeit, auf die Herrschende, Militärs sowie Diplomatinnen und Diplomaten autoritativen Einfluss üben konnten. Nach Shannon allerdings gelang es der Kryptographie, sich zu emanzipieren und in die Mitte des wissenschaftlichen Diskurses zu gelangen. Man könnte daher wohl auch sagen: Shannons Theorie vollzog für die Kryptographie die Transition vom Mythos zum Logos.

Nicht weniger bedeutsam war Shannons Theorie auch für den eher *klassischen* Bereich der Kryptographie, der allerdings uneingeschränkt bis heute Verwendung findet: die *symmetrische Kryptographie*. Das Paradigma Moderner Kryptographie machte in Kombination mit Digitalisierung und Kommerzialisierung auch davor keinen Halt und forderte gar das Selbstverständnis kryptographischer Forschung neu heraus. Retrospektiv lässt sich fragen: Wer würde es nach Shannon überhaupt wagen, Kryptographie nicht allein der Mathematik zu überlassen?

---

lichkeiten auch Mariusz Borowski und Marek Leśniewicz. „Modern usage of 'old' one-time pad". In: *2012 Military Communications and Information Systems Conference. Gdansk, Poland*. 2012, S. 1–5; im historischen Kontext auch Bauer, *Secret History*, S. 94–96.

29 Siehe zu einem Beweis und einer kurzen Diskussion Katz und Lindell, *Introduction to Modern Cryptography*, S. 35.

2.2 Der Data Encryption Standard (DES)

Die *National Security Agency* (NSA) ging aus der *Armed Forces Security Agency* (AFSA) hervor und wurde am 4. November 1952 durch eine Direktive des damaligen US-Präsidenten Harry S. Truman gegründet.[30] Zwei Missionsziele soll die Organisation verfolgen: „exploiting foreign communications, also known as Signals Intelligence (SIGINT), and protecting U.S. information systems, also called Information Assurance (IA)"[31]. Als Geheimdienstorganisation engagiert sich die NSA bis heute im Bereich der Überwachung, der Spionage und vor allem der Kryptographie.[32]

Insbesondere im Jahr 2013 rückte das Handeln der NSA auch in den internationalen öffentlichen Fokus, nachdem der US-amerikanische Whistleblower Edward Snowden Geheimdokumente veröffentlichen ließ.[33] Unter anderem ist dabei die systematische und umfassende Überwachung von US-Bürgerinnen und -Bürgern, ausländischen Personen, politischen Verbündeten und ganzen Onlinediensten dokumentiert.[34] Bereits fünfzig Jahre zuvor sah die NSA sich selbst, wie Steven Levy es nennt, als „the sole repository of cryptographic information in the country – not just that used by civilian government and all the armed forces, as the law dictated, but that used by the private sector as well"[35]. Mit Blick auf das vorherige Kapitel wird der Konflikt um Autorität und Mathematik deutlich: Die NSA „acted as if it actually owned mathematical truths"[36].

Sicherlich war die NSA zunächst tatsächlich lange Zeit alleiniger Hort für kryptographische Forschung. Der einstige Direktor der NSA, Bobby Inman, ging zum Beispiel davon aus, dass die NSA ein „monopoly on ta-

30 Siehe Kahn, *The Codebreakers*, S. 675; einführend im kryptographischen Kontext auch Bauer, *Secret History*, S. 345–378.

31 National Security Agency. *Transition 2001*. Dez. 2000. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3700340/National-Security-Agency-Transition-2001.pdf (besucht am 15.04.2024), S. 1.

32 Eine konzise Einführung im Kontext der Überwachung liefert hier Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3. Aufl. Indianapolis: Wiley, 2020, S. 922–925.

33 Siehe Edward Snowden. *Permanent Record*. London: Pan Books, 2019.

34 Zum Whistleblowing und Edward Snowden siehe Kapitel 7; dazu und zum Hintergrund insbesondere Glenn Greenwald. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Penguin Books, 2014.

35 Levy, *Crypto*, S. 15.

36 Ebd., S. 13.

lent“[37] gehabt habe. Die politische Macht der NSA bestand allerdings vor allem darin, Patentanfragen zu kontrollieren und jene Patente, die nicht in öffentliche Hände gelangen sollten, zu klassifizieren.[38] US-amerikanische Forschung zur Kryptographie war bis in die 1960er-Jahre also das, was sie historisch betrachtet meistens war: autoritativ kontrolliert, häufig einer bestimmten Organisation unterstellt – und die Forschungsleistungen sollten möglichst geheim bleiben.

Konnte eine solche Kryptographie dauerhaft erfolgversprechend sein? Gerade mit dem Beginn der Digitalisierung und einem globalen Internet? In einer Zeit, in der Kryptographie zudem nicht mehr nur eine militärische Angelegenheit war, sondern zunehmend auch eine ökonomisch-kommerzielle? Kerckhoffs hatte bereits im vorherigen Jahrhundert beschrieben, dass eine Veröffentlichung des kryptographischen Systems die Sicherheit des Systems nicht kompromittieren darf.[39] Heute auch als *Kerckhoffs' Prinzip* bezeichnet, meint dies, dass die Sicherheit des Systems lediglich auf der Geheimhaltung des Schlüssels beruhen darf. Jede Geheimdienstorganisation, die das Wissen, die Algorithmen, die Verfahren und die Anwendungen von Kryptographie unter Verschluss halten will, widerspricht daher diesem Prinzip.

Daher mag es wenig überraschend sein, dass diese menschengemachte Autorität über kryptographische Forschung und Nutzung in den kommenden Jahren sukzessive auf die Probe gestellt werden sollte. Kapitel 3 und Kapitel 4 werden näher auf die Zusammenhänge von Gesellschaft, Wissenschaft und Regulierung eingehen, bei denen letztlich auch ethische Konflikte zutage treten.[40] Für diesen Teil der Arbeit ist allerdings wichtig: Deskriptiv betrachtet war aufgrund von rasch fortschreitender Entwicklung des Computers sowie einer Kommerzialisierung von Kommunikation auch eine Weiterentwicklung von kryptographischen Verfahren für zivile Behörden und Unternehmen erforderlich. Die Probleme für die NSA begannen damit, dass ein kommerzieller Standard gefun-

37 Zitiert in ebd., S. 115.

38 Siehe ebd., S. 15.

39 Siehe dazu die Ausführungen in Abschnitt 1.1.

40 Gemeint ist hierbei z. B. das Motiv einer *Privacy-vs.-Sicherheit*-Dichotomie, die oftmals als Begründung für eine Art *notwendiger* Beschränkung von Kryptographie angesehen wird. Im späteren Verlauf wird allerdings argumentiert, dass eine solche Dichotomie weder der Realität noch einer ethischen Notwendigkeit entspricht; siehe Abschnitt 6.2.

den werden sollte, der eine solche Vertraulichkeit der Kommunikation gewährleisten sollte: der sogenannte *Data Encryption Standard* (DES).[41]

DES wurde als symmetrischer Verschlüsselungsalgorithmus am 15. Januar 1977 durch das *National Bureau of Standards* (NBS), den Vorgänger des heutigen *National Institute of Standards and Technology* (NIST), als *Federal Information Processing Standard 46* (FIPS 46) herausgegeben.[42] Dabei basiert der Algorithmus auf dem Verschlüsselungssystem *Lucifer*, das in den 1970er-Jahren durch den Kryptologen Horst Feistel bei IBM entwickelt worden war.[43] Auch bei Feistels Entwicklung wird deutlich, welchen Einfluss Claude Shannons Werk auf die Moderne Kryptographie hatte. Auf die Frage, woher Feistel die Ideen für sein Verschlüsselungssystem nahm, antwortete er: „The Shannon paper reveals it all."[44]

Lucifer war bereits auf dem US-amerikanischen Markt vertrieben worden, in einer geschwächten Version sogar weltweit.[45] Wie Lucifer ist DES eine sogenannte *Block Cipher*.[46] Dabei wird der Klartext in Blöcke unterteilt, die jeweils einzeln verschlüsselt werden. Auch die Entschlüsselung wird blockweise durchgeführt.[47] Entsprechend der fortschreitenden Digitalisierung nutzt DES auch kein natürlichsprachiges Alphabet mehr, sondern operiert nun auf Bits – genauer gesagt auf 64-Bit-Blöcken. Zur Verschlüsselung wird ein 56-Bit-Schlüssel verwendet, der insgesamt 16 Mal (in sogenannten *Runden*) auf den 64-Bit-Block angewandt wird. Dabei wird, ähnlich wie bei Shannon beschrieben, ein Netzwerk aus Substitution und Permutation verwendet. Wenn nun aber Shannons Theorie umfassend berücksichtigt wurde, wie konnte Lucifer beziehungsweise DES eine Kontroverse zur Sicherheit des Systems und zum Handeln der NSA auslösen?

41 Siehe zur historischen Einführung insbesondere Bauer, *Secret History*, S. 379–411.

42 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 169, allgemeiner auch S. 169–175; umfassender zur Geschichte auch Jarvis, *Crypto Wars*, S. 78–104.

43 Siehe ebd., S. 77–78 und 81.

44 Zitiert in Levy, *Crypto*, S. 45, siehe auch ebd., S. 44.

45 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 169.

46 Siehe dazu und zur folgenden Beschreibung von DES Katz und Lindell, *Introduction to Modern Cryptography*, S. 213–216. Siehe auch Dooley, *History of Cryptography and Cryptanalysis*, S. 169–173.

47 Die andere Art symmetrischer Verschlüsselung ist die *Stream Cipher*, bei der Ver- und Entschlüsselung kontinuierlich erfolgt und die an dieser Stelle nur der Vollständigkeit wegen genannt sein soll. Siehe weiterführend Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 20–21.

Im Fokus stand dabei zum einen die als zu kurz empfundene Schlüssellänge von nur 56 Bits, zumal Lucifer einen 128-Bit-Schlüssel verwendet hatte.[48] Um die Bedeutung der Schlüssellänge zu verstehen, hilft folgende Einordnung: Die Anzahl möglicher Schlüssel verdoppelt sich mit jedem weiteren Bit. Für einen 56 Bit langen Schlüssel gibt es insgesamt 2^{56} Möglichkeiten. Ein 128-Bit-Schlüssel allerdings lässt 2^{128} Möglichkeiten zu, also $2^{56} \cdot 2^{72}$. Schon damals gab es daher Stimmen, die den DES-Schlüssel als zu kurz empfanden.[49] Beispielsweise beschreibt Whitfield Diffie die Schlüssellänge bereits im Jahr 1975 als „at best barely adequate“[50]. Warum aber kam es trotzdem zu einem 56-Bit-Schlüssel? Eine mögliche Theorie war, dass die NSA auf IBM und das NBS eingewirkt hatte, da sie 56-Bit-Schlüssel brechen konnte.[51] Laut Dooley konnte dies allerdings nicht bewiesen werden.[52] Einige innerhalb von IBM sowie Forschende wie Diffie und Hellman sahen jedoch bereits damals eine Beeinflussung durch die NSA.[53] Später wurde bestätigt, dass IBM tatsächlich von der NSA überzeugt worden war, dass eine solche Schlüssellänge ausreichend sei.[54] Ob die Verkürzung der Schlüssellänge allerdings aus opportunistischen Gründen empfohlen wurde oder aber aus Performance- und Speichergründen, kann nicht mit abschließender Sicherheit festgestellt werden.

Die andere Kritik am Design von DES betraf die sogenannten *Substitutionsboxen*, auch *S-Boxen* genannt.[55] Die Analyse und die Prinzipien des Designs waren nicht veröffentlicht worden, und es wurde spekuliert, ob

48 Siehe Jarvis, *Crypto Wars*, S. 81–84; einführend auch Bauer, *Secret History*, S. 390–393.

49 Siehe Jarvis, *Crypto Wars*, S. 83–84, sowie Levy, *Crypto*, S. 37–39.

50 Whitfield Diffie. *Preliminary Remarks on the National Bureau of Standars Proposal Standard Encryption Algorithm for Data Protection*. Mai 1975. URL: https://stacks.stanford.edu/file/druid:wg115cn5068/1975%200522%20ltr%20to%20NBS.pdf (besucht am 15.04.2024), S. 3; auch zitiert in Jarvis, *Crypto Wars*, S. 84.

51 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 174.

52 Siehe ebd., S. 174.

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

54 Siehe United States Senate. *Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard*. Staff Report of the Senate Selected Committee on Intelligence. Washington: U.S. Government Printing Office, Apr. 1978. URL: https://www.intelligence.senate.gov/sites/default/files/publications/95nsa.pdf (besucht am 15.04.2024), S. 4; sowie Levy, *Crypto*, S. 63. Gleichzeitig stellt der Report fest, die NSA habe zertifiziert, dass DES nach ihrem besten Wissen frei von statistischen und mathematischen Schwächen sei.

55 Siehe einführend Bauer, *Secret History*, S. 393–395.

sich die NSA dadurch eine Hintertür (eine sog. *Backdoor*) für einen möglichen Zugriff auf die Kommunikation offen gelassen hatte.[56] Später jedoch wurden die tatsächlichen Gründe bekannt, warum die NSA Interesse an jener Geheimhaltung gehabt hatte: Die S-Boxen von DES verhindern eine bestimmte Art der Kryptoanalyse, die sogenannte *Differentielle Kryptoanalyse*.[57] Zum Zeitpunkt der Entwicklung von DES war die Differentielle Kryptoanalyse allerdings *nur* der NSA bzw. IBM bekannt. Dieses Wissen um eine neue Angriffsmethode wollte die Geheimdienstorganisation nicht mit den Überlegungen des Designs von DES veröffentlichen; gleichzeitig sollte DES gegen diese Differentielle Kryptoanalyse sicher sein – und daher entschied sich die NSA zur Geheimhaltung.[58] Es scheint plausibel, dass es sich tatsächlich nicht um eine Backdoor gehandelt hatte.

Egal, ob das Wirken der NSA nun rückblickend positiv, nachvollziehbar oder kritisch betrachtet wird: In jeglicher Hinsicht zeigt die Causa um DES auf, dass sich die Kryptographie im Umbruch befand. Eine Geheimhaltung von Designentscheidungen wurde nicht mehr ohne Weiteres von der wissenschaftlichen Forschung oder der Öffentlichkeit hingenommen. Die Intransparenz um die S-Boxen verringerte das Vertrauen in die Institution, und die Frage nach der Schlüssellänge war allenfalls kommunikativ undurchsichtig. Es handelte sich bei DES daher womöglich um den letzten größeren und gleichzeitig einigermaßen erfolgreichen Versuch der NSA, auf eine weit verbreitete Standardisierung von Kryptographie Einfluss zu nehmen. Für Levy steht fest: „DES was the NSA's first lesson that the new age of computer security was going to complicate its life considerably – perhaps even to the point of shaking the entire institution."[59]

An DES wird aber auch deutlich, dass die Zukunft der Standardisierung nicht mehr nur militärisch oder geheimdienstlich ausgerichtet war, sondern in zunehmendem Maße zivil und kommerziell.[60] So kam es, dass bereits 25 Jahre später und nach einigen prominenten DES-Entschlüsselungen kein Zweifel mehr daran bestand, dass DES durch einen Nachfol-

56 Siehe Jarvis, *Crypto Wars*, S. 83.

57 Siehe dazu und zum Folgenden Don Coppersmith. „The Data Encryption Standard (DES) and its strength against attacks". In: *IBM Journal of Research and Development* 38.3 (1994), S. 243–250.

58 Siehe Levy, *Crypto*, S. 55–56.

59 Ebd., S. 65.

60 Beispielhaft wird dies daran deutlich, dass die kommerziellen Interessen von IBM denen der NSA teilweise widersprachen, insbesondere was die Exportbeschränkungen betraf. Siehe Jarvis, *Crypto Wars*, S. 82–83.

ger abgelöst werden musste.[61] Dieses Mal allerdings sollte es nicht mehr die NSA sein, die weitreichend bei der Standardisierung mitwirkte, sondern allein das *National Institute of Standards and Technology* (NIST) – kein Geheimdienst also, sondern eine zivile US-Bundesbehörde.[62] Die Standardisierung der kryptographischen Forschung emanzipierte sich vom Einfluss des Geheimdienstes.

Der Ausschreibungsprozess für diesen neuen kryptographischen Standard verdeutlicht ein solches neuartiges Selbstverständnis der Modernen Kryptographie: Die Prinzipien und Überlegungen des Designs mussten vollständig veröffentlicht werden und die Schlüssellänge musste mindestens 128 Bits betragen.[63] Hinzu kam, dass zahlreiche Gruppen nicht aus den USA stammten, womit auch das *globale* Element der Modernen Kryptographie ans Tageslicht trat.[64] Schließlich wurde zum neuen Jahrtausend der von belgischen Wissenschaftlern entwickelte Algorithmus *Rijndael* als *Advanced Encryption Standard* (AES) auserkoren.[65]

Während DES noch mit stark technischen Methoden und Begriffen beschrieben worden war, erfolgte dies bei AES primär in mathematischen Formeln und Erklärungen.[66] Kryptographie steht seither auf dem Fundament der Mathematik. Allerspätestens mit AES war also der Paradigmenwechsel, zumindest im Bereich der symmetrischen Verschlüsselung, abgeschlossen. Die Bedeutung für militärische Akteure blieb zwar vorhanden, allerdings kam nun eben auch immer mehr die Bedeutung für kommerzielle und zivile Zwecke hinzu. Die autoritative Beeinflussung der Standardisierung musste daher reduziert werden.[67] Dass dies notwendig

61 Siehe zur Einführung in unterschiedliche Attacken auf DES Diffie und Landau, *Privacy on the Line*, S. 28–29. Siehe außerdem zum Wirken der Cypherpunks Jarvis, *Crypto Wars*, S. 92–99.

62 Siehe Dooley, *History of Cryptography and Cryptanalysis*, S. 175; außerdem einführend Diffie und Landau, *Privacy on the Line*, S. 249–251.

63 Siehe Levy, *Crypto*, S. 310. In der Praxis werden heute auch Schlüssel zur symmetrischen Verschlüsselung mit einer Länge von 256 Bit eingesetzt, die entsprechend 2^{256} verschiedene Schlüssel ermöglichen. Erfolgreiche Brute-Force-Attacken werden dadurch in der Praxis verhindert.

64 Siehe ebd., S. 310. Zumal es von den US-amerikanischen Teams lediglich eines gab, das nicht auch aus ausländischen Forschenden bestand; siehe Diffie und Landau, *Privacy on the Line*, S. 249.

65 Siehe ebd., S. 249–251.

66 Siehe ebd., S. 250.

67 Deutlich wird dies auch an späteren Ausschreibungsprozessen zur Standardisierung von Kryptographie, etwa bei dem Prozess zur Standardisierung von Post-Quanten-Kryptographie. Siehe Abschnitt 2.5.

und sinnvoll war, zeigt der Erfolg von AES: Auch zwanzig Jahre nach der Standardisierung ist keine Attacke bekannt, die AES hätte brechen können.

2.3 *Diffie-Hellman und RSA*

Mit AES konnte also ein symmetrisches Verschlüsselungsprotokoll entwickelt werden, das es zwei Parteien ermöglicht, durch einen gemeinsamen Schlüssel auch im digitalen Zeitalter sicher und vertraulich zu kommunizieren. Eine Problematik allerdings galt es noch zu lösen: Wie kann der *gemeinsame* Schlüssel von einem Kommunikationspartner zum anderen gelangen?[68] Wenn der Schlüssel über das Internet übertragen wird, müsste man davon ausgehen, dass er abgefangen werden kann. Böswillige Angreifende könnten damit die gesamte mit dem betreffenden Schlüssel verschlüsselte Kommunikation entschlüsseln. Man müsste somit diesen Schlüssel über einen zweiten, sicheren Kanal übertragen – allerdings ist dies im Internet wenig praktikabel. Alternativ könnte man sogenannte *Key Distribution Centers* oder *Trusted Third Parties* (TTP) nutzen, die jedoch in einem solch interdependenten Netzwerk unzählige Schlüssel zu verwalten hätten.[69]

Dieses Problem bezieht sich also auf die *Key Distribution* und den *Key Exchange*.[70] Die Herausforderung der Verwaltung von Schlüssels wird daher auch als *Key Management Problem* bezeichnet.[71] Seit Beginn der symmetrischen Verschlüsselung – von der Caesar-Chiffre über die Vigenère-Chiffre bis hin zu Enigma – waren diese Probleme weitgehend ungelöst.[72] Intuitiv betrachtet erscheint diese Situation womöglich auch

68 Siehe dazu und zum Folgenden Katz und Lindell, *Introduction to Modern Cryptography*, S. 359–360.

69 Siehe einführend zu möglichen Lösungen mithilfe von symmetrischen Verfahren Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 36–37. Siehe zu *Key Distribution Centers* Katz und Lindell, *Introduction to Modern Cryptography*, S. 361–363. Es wäre etwa aus ethischer Perspektive zu fragen, wer die Verantwortung für diese zentrale Instanz übernehmen sollte und wie sie kontrolliert werden könnte.

70 Siehe ebd., S. 359–360; außerdem Dooley, *History of Cryptography and Cryptanalysis*, S. 185–186.

71 Siehe Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 36.

72 Ausgenommen sind die oben genannten Alternativen, die jedoch wenig praktikabel sind.

ausweglos, denn irgendein Schlüssel *muss* ja übertragen werden – zumal seit Kerckhoffs feststeht, dass die Sicherheit des Systems ja gerade in der Geheimhaltung der Schlüssel liegen muss. Auch die US-amerikanischen Kryptographen Whitfield Diffie und Martin Hellman machten sich Gedanken über diese Fragen und Probleme.

In den 1970er-Jahren gelang ihnen schließlich die vielleicht bislang größte Revolution innerhalb der Kryptographie.[73] Ihre entscheidende Idee dabei war, mathematische Asymmetrien und eine sogenannte *Trapdoor-Einwegfunktion* (engl. *trapdoor one-way function*) im Bereich der Kryptographie zu nutzen.[74] Eine solche Trapdoor-Einwegfunktion basiert auf einem mathematischen Problem, im Fall von Diffie und Hellman auf dem *Problem des Diskreten Logarithmus*.[75] In einfachen Worten ausgedrückt kann eine Einwegfunktion in die eine Richtung *effizient* berechnet werden, in die andere Richtung allerdings nicht.[76] Mit der Trapdoor (dt. *Falltüre*) gibt es zusätzlich eine geheime Information, mit der die Einwegfunktion doch effizient umgekehrt werden kann.[77] Diffie und Hellman waren nun historisch die ersten, die eine Methode publiziert hatten, die dieses Wissen auf die Kryptographie anwendet.[78] Ihren Artikel *New Directions in Cryptography* leiteten sie 1976 daher auch mit einigem paradigmatischem Pathos ein: „We stand today on the brink of a revolution in cryptography."[79]

Was aber veränderte dieser Schlüsselaustausch ganz *prinzipiell*? Das Entscheidende ist, dass sich mit diesem Algorithmus zwei Parteien auch über einen unsicheren Kanal auf einen gemeinsamen Schlüssel einigen können. Dies gelingt also auch für den Fall, in dem eine böswillige Partei

73 Siehe einführend Katz und Lindell, *Introduction to Modern Cryptography*, S. 363–370, und Gathen, *CryptoSchool*, S. 42–48.

74 Siehe Diffie und Hellman, „New Directions in Cryptography", insbesondere S. 650. Siehe auch Katz und Lindell, *Introduction to Modern Cryptography*, S. 364, zu Einwegfunktionen zudem S. 332; sowie Beutelspacher, *Geheimsprachen und Kryptographie*, S. 52.

75 Siehe einführend Anderson, *Security Engineering*, S. 188–193.

76 Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 332.

77 Siehe Beutelspacher, *Geheimsprachen und Kryptographie*, S. 52.

78 Historisch wurden bereits wenige Jahre zuvor die Methoden am *Government Communications Headquarters* (GCHQ) entwickelt, jedoch nicht veröffentlicht; siehe dazu ausführlicher weiter unten. Außerdem wirkte auch Ralph Merkle in der Gruppe von Diffie und Hellman mit; siehe Singh, *The Code Book*, S. 256 und 270–272.

79 Diffie und Hellman, „New Directions in Cryptography", S. 644.

den Kanal passiv abhört.[80] Man benötigte damit keine zentrale Instanz mehr, die sich um das Management und die Verwaltung aller Schlüssel hätte kümmern müssen. Nun konnten zwei Parteien, zwei Individuen, vertraulich kommunizieren, ohne sich auf eine dritte Partei zu verlassen. Dieses revolutionäre Verfahren wird heute als *Diffie-Hellman-Schlüsselaustausch* (DH-Schlüsselaustausch) bezeichnet.

Das Key-Exchange-Problem schien damit zunächst gelöst.[81] Tatsächlich kann aber eine solche Kryptographie, die auch als *asymmetrische Kryptographie* oder *Public-Key-Kryptographie* bezeichnet wird, noch mehr erreichen: zum einen ein asymmetrisches System zur Ver- und Entschlüsselung;[82] zum anderen aber auch die Gewährleistung von Authentizität.[83] Für beides legten Diffie und Hellman die grundsätzlichen Ideen dar. Eine Public-Key-Kryptographie basiert darauf, dass $k_e \neq k_d$ ist.[84] Das bedeutet, der Schlüssel zur Verschlüsselung ist nicht identisch mit dem Schlüssel der Entschlüsselung. Entscheidend ist hierbei, dass es nicht möglich ist, k_d durch die Kenntnis von k_e zu ermitteln. Der Schlüssel k_d muss immer geheim bleiben, weshalb er auch *private key* genannt wird. k_e allerdings darf (und soll sogar) veröffentlicht werden – schließlich spielt es keine Rolle, ob auch andere Parteien Nachrichten mit diesem Schlüssel verschlüsseln können. Deswegen wird er auch als *public key* bezeichnet.[85]

80 Aktive Angriffe und sogenannte *man-in-the-middle attacks* sind jedoch möglich. Siehe weiterführend Katz und Lindell, *Introduction to Modern Cryptography*, S. 369–370.

81 Wie Peter Shor knapp zwanzig Jahre später zeigen konnte, gibt es einen Algorithmus, der den DH-Schlüsselaustausch (und einige andere asymmetrische Verfahren) bricht. Dieser benötigt allerdings einen Quantencomputer. Siehe Peter W. Shor. „Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *IEEE Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, S. 124–134; dazu auch Abschnitt 2.5.

82 Siehe Diffie und Hellman, „New Directions in Cryptography", S. 644. *Asymmetrisch* deswegen, weil der Schlüssel zur Verschlüsselung ein anderer ist als der zur Entschlüsselung.

83 Siehe ebd., S. 644–645. Siehe auch Dooley, *History of Cryptography and Cryptanalysis*, S. 189–191.

84 Der Schlüssel k_e dient zur Verschlüsselung, der Schlüssel k_d zur Entschlüsselung. Siehe zur Public-Key-Kryptographie im Folgenden einführend ebd., S. 189–191.

85 Der DH-Schlüsselaustausch wird also zur Einigung eines gemeinsamen Schlüssels verwendet, die Public-Key-Kryptographie zur Ver- und Entschlüsselung. Die sprachliche Unterscheidung ist allerdings unscharf.

Widerspricht dies nun Kerckhoffs' Prinzip, nach dem die Sicherheit des Systems nur darauf basiert, dass der Schlüssel geheim gehalten wird?[86] Tatsächlich lässt sich diese Frage nicht beantworten, denn Kerckhoffs' Ideen waren schließlich aus der Perspektive der symmetrischen Kryptographie entstanden. Eine Kryptographie, bei der *zwei* Schlüssel existieren, war für Kerckhoffs sicher nicht vorstellbar. Diese radikale Idee war in dem Sinne wohl auch eine Art „cryptographic heresy"[87]. Die asymmetrische Kryptographie eröffnet hier ein vollkommen neues Feld, das – wie für ein neues Paradigma üblich – auch nicht mit den Werkzeugen, Methoden und Hilfsmitteln des alten Paradigmas gedacht werden kann.

Das Problem der Authentizität war ebenfalls Teil dieses neuen Paradigmas. Über Jahrtausende war Kryptographie eine Frage vertraulicher Kommunikation. Nur jene Parteien können den Inhalt der Nachricht entschlüsseln, die es auch *sollen*. Mit dem Ziel der Authentizität dagegen soll nachgewiesen werden, dass die Nachricht wirklich von der Partei stammt, die der Absender zu sein vorgibt. Auch wenn Diffie und Hellman sowohl die Frage der Authentizität als auch die grundsätzlichen Ideen zur Public-Key-Kryptographie aufzeigten, lieferten sie dazu keinen konkreten Algorithmus. Dies gelang kurze Zeit später allerdings einer anderen Gruppe von Forschern: Ron L. Rivest, Adi Shamir und Leonard Adleman.[88]

Ihren Algorithmus, den sie in *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* darlegten, sahen sie als direkte Antwort auf den Artikel von Diffie und Hellman. Letztere hätten zwar, wie oben bereits erläutert, das Konzept vorgestellt, jedoch keine praktische Implementierung.[89] Die grundlegende Notwendigkeit für solch ein System sahen sie im Aufkommen der E-Mail, die ähnliche Eigenschaften wie Papierpost erfüllen muss: Einerseits müssen Nachrichten *vertraulich* sein, andererseits müssen sie *signiert* werden können.[90] Ähnlich wie der

86 Horst Feistel, Entwickler von *Lucifer*, erklärte in einem eiligen Moment, dass ein öffentlicher Schlüssel Kerckhoffs' zweitem Grundsatz widersprechen würde. Siehe Levy, *Crypto*, S. 75.

87 Jarvis, *Crypto Wars*, S. xvi.

88 Siehe Ron L. Rivest, Adi Shamir und Leonard Adleman. „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Communications of the ACM* 21.2 (1978), S. 120–126.

89 Siehe ebd., S. 120.

90 Siehe ebd., S. 120. Diffie und Hellman nennen Ersteres *privacy problem* und Letzteres *authentication problem*. Siehe Whitfield Diffie und Martin E. Hellman. „Privacy and

DH-Schlüsselaustausch basiert auch der Algorithmus von Rivest, Shamir und Adleman, der gemäß den Initialen als *RSA* abgekürzt wird, auf einer Einwegfunktion.

Das mathematische Problem ist bei RSA jedoch das sogenannte *Faktorisierungsproblem*.[91] Um dies an einem einfachen Beispiel zu beschreiben: Ein klassischer Computer kann die Berechnung $7 * 3 = 21$ effizient ausführen; für die Faktorisierung der zwei Primzahlen 7 und 3 ausgehend von der Zahl 21 ist jedoch ein proportional deutlich größerer Rechen- und Zeitaufwand notwendig.[92] Für den genauen Algorithmus sei auf die zahlreiche Standardliteratur verwiesen, schematisch funktioniert RSA jedoch folgendermaßen: Wenn Alice (Partei A) eine Nachricht an Bob (Partei B) schicken möchte, dann generiert Bob zunächst ein Schlüsselpaar, das aus einem *private key* k_d^{Bob} und einem *public key* k_e^{Bob} besteht. Der *public key* k_e^{Bob} wird daraufhin veröffentlicht, beispielsweise über ein Repository im Internet. Alice nutzt nun Bobs *public key* k_e^{Bob} und verschlüsselt damit ihre Nachricht. Die verschlüsselte Nachricht kann Alice anschließend an Bob senden. Dies kann auch über einen unsicheren Kanal geschehen, denn ausschließlich Bob kann nun die Nachricht mit seinem geheim gehaltenen *private key* k_d^{Bob} entschlüsseln.[93]

Mit diesem Verfahren kann auch das Authentizitäts-Problem gelöst werden.[94] Gehen wir davon aus, dass nun Bob eine signierte Nachricht an Alice senden möchte.[95] Dazu nutzt Bob seinen *private key* k_d^{Bob}, signiert damit die Nachricht und sendet sie anschließend an Alice. Alice kann nun mit Bobs *public key* k_e^{Bob} überprüfen, ob die Nachricht wirklich von Bob stammt, denn niemand anderes hätte die Nachricht mit Bobs *private key* k_d^{Bob} signieren können. Alice kann dann also sicher sein, dass die

Authentication: An Introduction to Cryptography". In: *Proceedings of the IEEE* 67.3 (1979), S. 397–427, hier S. 398.

91 Siehe Rivest, Shamir und Adleman, „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"; weiterführend auch Katz und Lindell, *Introduction to Modern Cryptography*, S. 410–433; historisch Dooley, *History of Cryptography and Cryptanalysis*, S. 192–193.

92 In der Praxis sind die Zahlen sehr viel größer. Siehe zum Faktorisierungsproblem Anderson, *Security Engineering*, S. 185–188.

93 Vorausgesetzt ist hierbei natürlich, dass Bob seinen *private key* k_d^{Bob} auch wirklich geheim hält.

94 Siehe dazu und zu digitalen Signaturen umfassend Katz und Lindell, *Introduction to Modern Cryptography*, S. 439–486.

95 Zur Vereinfachung gehen wir davon aus, dass dies dieses Mal unverschlüsselt stattfinden soll.

Nachricht nicht von einer böswilligen Partei stammt.[96] Man spricht daher von *digitalen Signaturen*. Auch hier funktioniert dieses Verfahren nur aufgrund des mathematischen Faktorisierungsproblems sowie der Beziehung von *private key* k_d und *public key* k_e.[97]

Sowohl der DH-Schlüsselaustausch als auch RSA waren wahrliche Meilensteine der Kryptographiegeschichte – sowohl aus theoretischer als auch aus praktischer Perspektive.[98] Bis heute spüren wir tagtäglich und ubiquitär die Folgen dieser Entwicklung. Reg Whitaker bezeichnet die Public-Key-Kryptographie gar als „the end of the state's monopoly and the democratization of encryption"[99]. Und für Craig Jarvis war die Public-Key-Kryptographie zusammenfassend mehr eine Entdeckung als eine Erfindung:

> For it was a discovery, rather than an invention. Diffie und Hellman's public key cryptography was to computer science as Newton's theory of universal gravitation was to physics, as Pasteur's germ theory had been to medicine, and as Darwin's theory of evolution was to biology.[100]

Die asymmetrische Kryptographie kann damit zu Recht als ein Pfeiler des Paradigmenwechsels von der Klassischen Kryptographie hin zu einer Modernen Kryptographie gelten. Auch Naccache, Ryan und Quisquater kommen zu einer solchen Rezeption – denn das Revolutionäre ist ja gerade, dass die Fähigkeit zum *Verschlüsseln* nun nicht mehr gleichzeitig auch die Fähigkeit zum *Entschlüsseln* bedeuten muss:

> The discovery in the 1970s of public key cryptography revolutionized the subject and brought it out of the shadows. The realization that the ability to encrypt does

96 Wieder angenommen, nur Bob hat Zugriff auf seinen *private key*.

97 Siehe einführend auch Anderson, *Security Engineering*, S. 185–188.

98 Einer breiteren Öffentlichkeit bekannt wurde diese Art der Kryptographie bereits 1977 durch Martin Gardners Artikel in *Scientific American*; siehe Martin Gardner. „Mathematical Games: A new kind of cipher that would take millions of years to break". In: *Scientific American* (Aug. 1977), S. 120–124. Auch einige der späteren Cryptoaktivistinnen und -aktivisten sind gerade durch diesen Artikel auf die Bedeutung der asymmetrischen Kryptographie aufmerksam geworden. Siehe Thomas Rid. *Rise of the Machines: The Lost History of Cybernetics*. Melbourne und London: Scribe, 2016, S. 252–253 und 262.

99 Reg Whitaker. *The End of Privacy: How Total Surveillance Is Becoming Reality*. New York: The New Press, 1999, S. 108.

100 Jarvis, *Crypto Wars*, S. xvi.

> not necessarily entail the ability to decrypt overturned (implicit) assumptions that had held sway for centuries. Arguably this insight is comparable in its impact on cryptography as that of Einstein's Theory of Relativity, with the realization that space is not absolute, on physics.[101]

Und obwohl Diffie und Hellman sowie Rivest, Shamir und Adleman am meisten Anerkennung für diese Entdeckungen erhalten, weiß man heute, dass diese grundsätzlichen Algorithmen bereits wenige Jahre zuvor auch auf der anderen Seite des Globus entdeckt wurden.[102] Am *Government Communications Headquarters* (GCHQ), dem UK-Pendant zur US-amerikanischen NSA, hatten zunächst James Ellis, dann Clifford Cocks und schließlich Malcolm Williamson solche Lösungen entwickelt. Trotzdem sind es nicht Ellis, Cocks und Williamson, nach denen die Public-Key-Kryptographie benannt wurde. Der Grund dafür ist simpel: Ihnen wurde verboten, darüber zu sprechen. Erst im Dezember 1997 durfte Cocks öffentlich zum ersten Mal davon berichten. Und Ellis, Cocks und Williamson erfuhren rückblickend Anerkennung für ihr Wirken als die eigentlich ersten Entdecker der Public-Key-Kryptographie.[103]

2.4 Kryptographie und Informationssicherheit

In der Klassischen Kryptographie war das Ziel der Kryptographie maßgeblich die Verschlüsselung von Kommunikation. Nachrichten sollten nur von denen entschlüsselt werden können, die dazu auch autorisiert sind. Im Paradigma der Modernen Kryptographie kommen nun weitere Ziele hinzu. So wird etwa die asymmetrische Kryptographie für die Verschlüsselung *und* für die Gewährleistung von Authentizität genutzt. Und auch die asymmetrische Kryptographie wird in der Praxis oft zusammen mit symmetrischen Verschlüsselungsverfahren und sogenannten Hash-Algorithmen verwendet, wodurch Vertraulichkeit und Integrität einer Nachricht sichergestellt werden soll. Mit all diesen Verfahren wer-

101 Naccache, Ryan und Quisquater, „Preface".

102 Siehe dazu und zu diesem Absatz Dooley, *History of Cryptography and Cryptanalysis*, S. 190–191; ausführlicher auch Levy, *Crypto*, S. 313–330, sowie Rid, *Rise of the Machines*, S. 248–250.

103 Siehe umfassender Singh, *The Code Book*, S. 279–292.

den sogenannte *Schutzziele* der Informationssicherheit verfolgt.[104] Solche Schutzziele „sind Sicherheitsanforderungen, die an ein System gestellt werden und die durch die Sicherheitseigenschaften des Systems schlussendlich zu gewährleisten sind"[105]. Unterteilt werden diese Schutzziele meist in *Vertraulichkeit* (engl. *confidentiality*), *Integrität* (engl. *integrity*) und *Verfügbarkeit* (engl. *availability*), sodass sie im Englischen mit *CIA* abgekürzt werden.[106] Hinzu kommen weitere Schutzziele wie *Rechtsverbindlichkeit/Nicht-Abstreitbarkeit* (engl. *non-repudiation*) und *Zurechenbarkeit* (engl. *accountability*).[107] Für die Kryptographie ist insbesondere auch das Schutzziel der *Authentizität* (engl. *authenticity*) von Bedeutung.[108] Letzteres ist aus ethischer Sicht primär im Fall von Identifikation und Identifizierbarkeit relevant, wie Abschnitt 7.3 zeigen wird.

Wenn also Moderne Kryptographie heute mehr zum Ziel hat als nur vertrauliche Kommunikation, dann sollte auch eine *Ethik der Kryptographie* diese anderen Facetten und Anwendungen nicht außer Acht lassen.[109] Eine Systematisierung anhand von Schutzzielen hilft dabei einer ethischen Analyse, Zielkonflikte zu identifizieren und Rahmenbedingungen für eine ganzheitliche Informationssicherheit zu etablieren. Beispielsweise muss eine Bank sicherstellen, dass Transaktionen vertraulich und privat sind. Gleichzeitig muss sie sich aber auch auf die Authentizität der Nachrichten und der Nutzenden verlassen können, damit die Transaktion die intendierte Partei erreicht. Damit die Transaktion zudem

104 Über das Verhältnis der Kryptographie zu Schutzzielen siehe Yvo Desmedt. „What is the Future of Cryptography?" In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Berlin und Heidelberg: Springer, 2016, S. 109–122.

105 Eckert, *IT-Sicherheit*, S. 2. Siehe zu den folgenden Schutzzielen auch Oorschot, *Computer Security and the Internet*, S. 2–3.

106 Siehe Eckert, *IT-Sicherheit*, S. 9–12; aus rechtlicher Perspektive auch Marcus Heinemann. *Grundrechtlicher Schutz informationstechnischer Systeme: Unter besonderer Berücksichtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Berlin: Duncker & Humblot, 2015, S. 73–75.

107 Siehe Eckert, *IT-Sicherheit*, S. 12–13, sowie Armin Lunkeit und Wolf Zimmer. *Security by Design: Security Engineering informationstechnischer Systeme*. Berlin und Heidelberg: Springer Vieweg, 2021, S. 89; aus rechtlicher Perspektive auch Heinemann, *Grundrechtlicher Schutz informationstechnischer Systeme*, S. 76–78.

108 Siehe Eckert, *IT-Sicherheit*, S. 9.

109 Siehe beispielsweise Konstantinos Limniotis. „Cryptography as the Means to Protect Fundamental Human Rights". In: *Cryptography* 5.4 (2021).

integer bleibt, darf der Betrag der Transaktion nicht verändert werden. All dies sind zunächst grundsätzliche Fragen der Informationssicherheit. Die Kryptographie allerdings ist das Werkzeug, mit dem diese Schutzziele der Informationssicherheit erreicht werden können. Im Folgenden soll auf die einzelnen Schutzziele eingegangen und deren Verhältnis zur Kryptographie bestimmt werden.

Vertraulichkeit

Mit dem Schutzziel der Vertraulichkeit ist beschrieben, dass nicht-öffentliche Informationen nur autorisierten Parteien zugänglich sein sollen.[110] Autorisierung meint hierbei, dass diese Partei Zugriffsrechte auf die betreffenden Informationen besitzt.[111] Dieses Schutzziel deckt sich also mit dem, was bereits die Klassische Kryptographie zum Ziel hatte: Nur jene Personen oder Systeme sollen die Möglichkeit haben, die Informationen unverschlüsselt zu lesen, die dazu auch autorisiert sind.[112] Systematisch unterschieden werden bei der Vertraulichkeit zwei Anwendungsebenen: einerseits eine *zeitliche* Ebene und andererseits eine *räumliche* Ebene.[113] *Zeitlich* meint, dass Informationen und Daten über einen gewissen Zeitraum zu schützen sind, etwa auf einer lokalen Festplatte oder bei ausgedruckten Dokumenten. Die *räumliche* Ebene bezieht sich dagegen auf die technologische Kommunikation. Wenn Alice in Paris mit Bob in Hongkong kommuniziert, dann möchten beide Parteien, dass keine dritte Partei von den Inhalten Kenntnis erlangen kann.[114]

110 Siehe einführend Oorschot, *Computer Security and the Internet*, S. 3. Für eine rechtliche Perspektive zur Vertraulichkeit siehe Heinemann, *Grundrechtlicher Schutz informationstechnischer Systeme*, insbesondere S. 74–75 und 79.

111 Siehe zu Autorisierung Eckert, *IT-Sicherheit*, S. 5. Zu unterscheiden ist hierbei die *Authentifizierung*, dazu weiter unten. Auf andere Art formuliert meint Autorisierung die Bindung einer Identität an eine Menge zulässiger Aktionen; siehe Lunkeit und Zimmer, *Security by Design*, S. 44.

112 Selbst Kahn definiert die Kryptographie noch wie folgt: „The methods of cryptography […] render [a message] unintelligible to outsiders by various transformations of the plaintext." Kahn, *The Codebreakers*, S. xv.

113 Siehe dazu und zum Folgenden Katz und Lindell, *Introduction to Modern Cryptography*, S. 5–6. Katz und Lindell beschreiben diese zwei Anwendungen im Rahmen einer, wie sie es nennen, *Private-Key-Kryptographie*, die allerdings deckungsgleich ist mit einer symmetrischen Kryptographie.

114 Eine weitere Frage wäre hier, ob bereits das Wissen, dass Alice mit Bob kommuniziert, unter das Schutzziel der Vertraulichkeit fallen sollte. Diese Differenzierung

Die Maßnahmen zur Wahrung von Vertraulichkeit sind abhängig von der konkreten Nutzungssituation. In der brieflichen Kommunikation soll die Vertraulichkeit des Inhalts beispielsweise durch das Briefgeheimnis oder einen Briefumschlag gewahrt werden. Digitalisiert spielen kryptographische Systeme eine entscheidende Rolle.[115] Kryptographische Verfahren können beispielsweise im Kontext von Festplattenverschlüsselung Vertraulichkeit gewährleisten, wenn symmetrische Algorithmen wie AES verwendet werden.[116] Eine vertrauliche räumliche Kommunikation kann durch ein asymmetrisches Verfahren wie den DH-Schlüsselaustausch erreicht werden. Sobald beide Parteien einen gemeinsamen Schlüssel haben, kann dieser für eine symmetrische Verschlüsselung genutzt werden.[117]

Integrität

Mit dem Schutzziel der Integrität sollen Daten unverändert bleiben, außer wenn die Änderungen autorisiert sind.[118] Dazu werden zum einen Methodiken der Fehlererkennung und Fehlerbehebung genutzt, zum anderen auch Zugangskontrollen sowie kryptographische Prüfsummen.[119] Für Zugangskontrollen sind vor allem Rechte wie Schreib- und Leserechte festzulegen.[120] Kryptographische Prüfsummen (engl. *cryptographic checksums*) hingegen erlauben eine Erkennung von veränderten Daten *a posteriori*, wobei in der Praxis sogenannte Hashfunktionen verwendet werden.[121] Sowohl bösartige Angriffe als auch unbeabsichtigte Fälle von

zeigt den Unterschied von *Inhaltsdaten* und *Metadaten*, worauf an späterer Stelle noch eingegangen wird.

115 Darüber hinausgehend wären z. B. auch Möglichkeiten der Zugriffskontrolle zu nennen; siehe Oorschot, *Computer Security and the Internet*, S. 3.

116 Die Schlüssel dürfen dabei natürlich nur den autorisierten Personen zugänglich sein.

117 In der Praxis ist eine möglichst nachweisbare Gewährleistung einer kryptographischen Implementierung komplexer. So sind unter anderem Implementierungsdetails zu berücksichtigen, die beispielsweise *Seitenkanal-Angriffe* (engl. *side-channel attacks*) verhindern sollen. Desmedt fragt daher auch, inwieweit wir Implementierungen vertrauen können; siehe Desmedt, „What is the Future of Cryptography?", S. 113, zur Einführung S. 113–114.

118 Siehe einführend Oorschot, *Computer Security and the Internet*, S. 3.

119 Siehe ebd., S. 3.

120 Siehe Eckert, *IT-Sicherheit*, S. 9.

121 Siehe ebd., S. 9–10. Einführend zu Hashfunktionen auch Anderson, *Security Engineering*, S. 152–154, 157–161 und 181–185, und Bauer, *Secret History*, S. 498–504.

beispielsweise Übertragungsfehlern sollen dadurch identifiziert und korrigiert werden können. In der brieflichen Kommunikation wird Integrität hingegen durch eine Versiegelung der Nachricht erreicht. Eine Veränderung der Nachricht kann also angenommen werden, wenn das Siegel gebrochen wurde.

Die Entwicklung der grundsätzlichen Prinzipien solcher Hashfunktionen reicht weit über das digitale Zeitalter zurück. So sahen sich in der Mitte des 19. Jahrhunderts Banken vor die Herausforderung gestellt, Authentizität und Integrität trotz telegraphischer Kommunikation zu wahren.[122] Dafür wurden *test codes* entwickelt, wodurch eine Veränderung der übermittelten Nachricht detektiert, gleichzeitig aber nichts über den Inhalt der Nachricht verraten wurde. Es handelte sich damals wie heute um die Idee einer *Einwegfunktion* (engl. *one-way function*).[123]

Auch wenn die Anwendungsidee von Prüfsummen und Hash-Algorithmen bereits historisch einige Zeit zurückliegt, lässt sich auch hier das Paradigma der Modernen Kryptographie erkennen: Hash-Algorithmen sind heute Teil der Mathematik und Informatik. Daher werden, ähnlich wie bei der symmetrischen Verschlüsselung, standardisierte Verfahren verwendet, die ein deutlich höheres Maß an Sicherheit gewährleisten können. Als Beispiel kann der *Secure Hash Algorithm 3* (SHA-3) genannt werden.[124]

Verfügbarkeit

Mit dem Schutzziel der Verfügbarkeit ist beschrieben, dass Informationen, Dienste und Ressourcen für autorisierte Zugriffe zugreifbar bleiben.[125] Bösartige Parteien, die gegen dieses Schutzziel handeln, führen sogenannte *Denial-of-Service*-(DoS-) bzw. *Distributed-Denial-of-Service*-(DDoS-)Angriffe durch.[126] Solche Angriffe sollen etwa einen Webserver durch eine massive

122 Siehe dazu und zur folgenden Historie Anderson, *Security Engineering*, S. 152–154.
123 Bereits 1678 war eine solche Einwegfunktion entwickelt worden; siehe ebd., S. 153.
124 Siehe einführend Katz und Lindell, *Introduction to Modern Cryptography*, S. 235–236.
125 Siehe Oorschot, *Computer Security and the Internet*, S. 3. In komplexen Systemen kann eine Verzögerung bis zu einem gewissen Grad erwartbar sein. Wie Eckert daher erkennt, ist für das Schutzziel der Verfügbarkeit die Trennlinie von autorisierten und unautorisierten Aktionen ungenau; siehe Eckert, *IT-Sicherheit*, S. 12.
126 Siehe Oorschot, *Computer Security and the Internet*, S. 3.

Flut von Anfragen zur Abschaltung zwingen. Das Erreichen des Schutzziels der Verfügbarkeit kann aber auch durch sogenannte *Ransomware*-Attacken verhindert werden. Zusammengesetzt aus den Begriffen *ransom* (dt. *Lösegeld*) und *software* bezeichnet der Begriff Programme, die sich in den Computersystemen der Angegriffenen einnisten und diese verschlüsseln. Als kryptographische Verfahren werden oft RSA in Kombination mit AES genutzt.[127] Die Opfer werden im Anschluss mit einer Lösegeldforderung konfrontiert, um die Systeme wieder entschlüsseln zu können. Eine Garantie, dass eine Entschlüsselung anschließend auch tatsächlich stattfindet, haben die Angegriffenen jedoch nicht.

Einer breiten Öffentlichkeit bekannt wurde Ransomware durch den Wurm *WannaCry* im Jahr 2017.[128] So wurden etwa auch Krankenhäuser und Teile der kritischen Infrastruktur Opfer dieser Attacken.[129] Mit der Nachricht *Oops, your files have been encrypted!* wurden Nutzende aufgefordert, innerhalb von drei Tagen 300 US-Dollar in der Kryptowährung *Bitcoin* als Lösegeld zu bezahlen. Wer diese erste Forderung nicht erfüllte, dessen Lösegeldforderung wurde verdoppelt. Nach sieben Tagen sollten die verschlüsselten Dateien endgültig gelöscht werden. Betroffen waren hierbei innerhalb weniger Tage über 300.000 Nutzende weltweit.[130]

Das Verhältnis zur Kryptographie ist hier aber komplexer, als auf den ersten Eindruck angenommen werden könnte. Denn für all diese Angriffe können nicht allein die Kryptographie respektive die Möglichkeiten, die sich durch die Kryptographie ergeben, verantwortlich gemacht werden. Zum einen liegen die Ursachen für den Erfolg von Ransomware an anderer Stelle, zum Beispiel an fehlenden Sicherheitskopien, ungeschützten Netzwerken oder veralteter Software. Zum anderen kann die Kryptographie auch bei Ransomware Vertraulichkeit sicherstellen. Eine Drohung

127 Siehe Aaron Zimba und Mumbi Chishimba. „On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems". In: *European Journal for Security Research* 4.1 (2019), S. 3–31, hier S. 27.

128 Siehe Maria F. Prevezianou. „WannaCry as a Creeping Crisis". In: *Understanding the Creeping Crisis*. Hrsg. von Arjen Boin, Magnus Ekengren und Mark Rhinard. Cham: Palgrave Macmillan, 2021, S. 37–50. Siehe zur Ökonomie hinter Ransomware Zimba und Chishimba, „On the Economic Impact of Crypto-ransomware Attacks". Ein anderes Beispiel für Ransomware ist der sogenannte *Gpcode*, der sich ab 2006 verbreitete; siehe Eckert, *IT-Sicherheit*, S. 23–24.

129 Siehe dazu und zum Folgenden Prevezianou, „WannaCry as a Creeping Crisis", S. 38.

130 Siehe Zimba und Chishimba, „On the Economic Impact of Crypto-ransomware Attacks", S. 15.

mit der Veröffentlichung von gestohlenen Daten läuft ins Leere, wenn die betreffenden Daten bereits zuvor sicher und vertraulich verschlüsselt worden sind.

Authentizität

Authentizität ist „die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar ist“[131]. Der Prozess der Überprüfung nennt sich Authentifikation.[132] In der brieflichen Kommunikation wird Authentizität etwa durch eine Unterschrift ermöglicht, die mit vorher signierten Unterlagen verglichen werden kann. In der digitalen Welt dagegen lässt sich das Schutzziel der Authentizität insbesondere mit *Public-Key Infrastructures* (PKI) lösen. Dabei werden digitale Signaturen genutzt, die die Nachrichten eindeutig einem Subjekt zuordnen. In der Praxis nutzt Alice ihren *private key* zur Signierung einer Nachricht. Bob kann anschließend die Signatur mit dem *public key* von Alice überprüfen. Im engeren Sinne ist die Authentizität von der *Identifizierung* zu unterscheiden. Die Identifizierung ermittelt eine Identität aus den verfügbaren Informationen, ohne dass zuvor eine ausdrückliche Identität beteuert worden ist.[133] Gleichwohl können in der Konsequenz Authentifizierung und Identifizierung zusammenhängen. Damit verbunden ist selbstverständlich auch die Frage nach der Rechtsverbindlichkeit und der Zurechenbarkeit.

Rechtsverbindlichkeit & Zurechenbarkeit

Die Schutzziele Rechtsverbindlichkeit und Zurechenbarkeit sind dann gegeben, wenn es unmöglich ist, im Nachhinein die Durchführung einer Aktion abzustreiten, und wenn damit eine Entität für eine vergangene

131 Eckert, *IT-Sicherheit*, S. 8.

132 Siehe ebd., S. 8. Nach Lunkeit und Zimmer wird im deutschen Sprachraum zwischen Authentifikation und Authentifizierung unterschieden; siehe Lunkeit und Zimmer, *Security by Design*, S. 44. Im Deutschen kommt zudem der Begriff *Authentisierung* hinzu. Eine ausführliche Analyse der deutschen Begrifflichkeiten würde an dieser Stelle zu weit gehen und ist nicht im Sinne der Arbeit. Zur Vereinfachung orientiert sich die Diskussion daher am englischen Begriff der *authentication*.

133 Siehe Oorschot, *Computer Security and the Internet*, S. 56.

Aktion verantwortlich gemacht werden kann.[134] In der Praxis wird dies neben digitalen Signaturen auch durch Logging oder Transaktionsbeweise erreicht.[135] Insbesondere in Handels- und Rechtssituationen spielt dieser Aspekt eine hervorgehobene Rolle.[136] Allerdings sind diese Schutzziele nicht immer erstrebenswert. So steht *Anonymität* der Zurechenbarkeit entgegen.[137] Differenzierung ist hierbei jedoch insofern erforderlich, als es sich bei den meisten Diskussionen um Anonymität um die ungewollte Zurechnung zur *personellen* und *öffentlichen* Identität handelt. Ein Maß an *technischer* Zurechenbarkeit ist auch in Netzwerken, die eine solche Form der Anonymität wahren möchten, für einen Kommunikationsaustausch notwendig und gewollt.[138]

Jedes einzelne Schutzziel beschreibt somit wünschenswerte und ggf. erforderliche Rahmenbedingungen von sicheren Systemen. Trotzdem können sich Schutzziele auch widersprechen. Wenn ein Backup eines Systems offline gespeichert wird, erhöht dies die Vertraulichkeit. Niemand kann, ohne vor Ort zu sein, auf das Backup zugreifen. Physische Barrieren wie ein Tresor können die Vertraulichkeit weiter erhöhen. All dies senkt aber auch die Verfügbarkeit, denn auf das Backup kann es keinen Fernzugriff per Internet mehr geben. Andere Schutzziele hingegen können situativ komplementär und in Kombination umgesetzt werden, etwa Integrität in Verbindung mit Authentizität. Dies kann erreicht werden, indem der Hashwert einer Nachricht mit einem *private key* signiert wird.

Einer der bedeutendsten Anwendungsfälle der Informationssicherheit und mit ihr der Kryptographie ist heute das Internet und das World Wide Web. In Kapitel 4 wird dediziert das regulatorische Verhältnis von

134 Siehe ebd., S. 4, sowie Eckert, *IT-Sicherheit*, S. 12.

135 Siehe Oorschot, *Computer Security and the Internet*, S. 4.

136 Siehe Eckert, *IT-Sicherheit*, S. 12.

137 Anonymität ist definiert als „the property that one's actions or involvement are not linkable to a public identity"; Oorschot, *Computer Security and the Internet*, S. 4. Im Deutschen: „Unter der Anonymisierung versteht man das Verändern personenbezogener Daten der Art, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können"; Eckert, *IT-Sicherheit*, S. 13.

138 Beispielsweise verschleiern anonyme Netzwerken wie *Tor* die Verbindung von digitalen Identitäten zu öffentlichen Identitäten. Aus technischer Perspektive ist jedoch auch hier ein Maß an Zurechenbarkeit und Verbindlichkeit für den Kommunikationsaustausch selbst notwendig.

Kryptographie und Internet analysiert werden, weswegen wir uns hier auf eine rein technologische Sicht beschränken können. Im Internet wird Sicherheit und Verschlüsselung nämlich nicht direkt durch die physische Infrastruktur erreicht, sondern durch eine Protokollentwicklung auf Transport- und Anwendungsebene.[139] Einer der dabei wichtigsten Standards ist *HTTPS* – das *Hypertext Transfer Protocol Secure*.[140] HTTPS baut dabei grundsätzlich auf HTTP auf, verwendet jedoch zusätzlich das *SSL*- bzw. *TLS*-Verfahren.[141] Mit einer Kombination unterschiedlicher kryptographischer Verfahren können mit HTTPS die Schutzziele der Vertraulichkeit, Integrität und Authentizität auch im World Wide Web erreicht werden. Ohne solche Protokollentwicklungen, die auf der Modernen Kryptographie basieren, wäre das Internet ein unsicheres Kommunikationsnetzwerk.

Ein anderer, immer relevanter werdender Fall ist das *Internet-of-Things* (IoT), bei dem Endgeräte mit dem Internet verbunden sind und miteinander kommunizieren können. Ein IoT-Gerät ist zum Beispiel eine Smartwatch, die mit dem Internet sowie mit dem Mobiltelefon verbunden ist. Auch wenn solche Geräte das alltägliche Leben an vielen Stellen bereichern, können sie für entscheidende Sicherheitsprobleme sorgen.[142] Dies ist unter anderem deswegen relevant, weil sie ob ihrer Natur oftmals in privaten und intimen Bereichen eingesetzt werden – zum Beispiel eine Kamera, die spielende Kinder im Garten filmt, ein Kühlschrank, der die Essgewohnheiten von Personen dokumentiert und auswertet, sowie ein im Schlafzimmer stehender *smarter* Lautsprecher,

139 In Kapitel 4 wird das zugrundeliegende *End-to-End Principle* näher diskutiert werden.

140 Siehe dazu und zum Folgenden einführend Oorschot, *Computer Security and the Internet*, S. 252–254; zu TLS auch Anderson, *Security Engineering*, S. 195–197.

141 SSL bedeutet *Secure Sockets Layer*, der Nachfolger TLS ist die Abkürzung für *Transport Layer Security*.

142 Siehe im Kontext von Cyber Threats beispielsweise Richard A. Clarke und Robert K. Knake. *The Fith Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press, 2019, S. 265–280; im Kontext des *Going Dark*-Problems, das Kapitel 6 diskutieren wird, siehe zudem Urs Gasser u. a. *Don't Panic: Making Progress on the "Going Dark" Debate*. Berkman Center for Internet & Society at Harvard University, 1. Feb. 2016. URL: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (besucht am 15.04.2024).

der sowohl das Schnarchen als auch alle anderen Tätigkeiten mithören wird.[143]

Zusammenfassend zeigt sich im Kontext von Informationssicherheit und Kryptographie, dass die Verschlüsselung hinsichtlich der Vertraulichkeit *ein* bedeutendes Schutzziel darstellt. Vertraulichkeit und Geheimhaltung von Informationen sind das, was eine systematische Kryptographie seit jeher zum Ziel hatte. Die folgenden Kapitel werden sich daher maßgeblich mit Fragen der *Verschlüsselung* auseinandersetzen. Ethische Fragen, die dabei auftreten, sind zum Beispiel: Wer oder was soll vertraulich kommunizieren dürfen? Welche Eingriffsrechte sollten staatliche Strafverfolgungsbehörden erhalten? Welche Konsequenzen sind zu befürchten, wenn Unternehmen das Ziel der Vertraulichkeit ungenügend umsetzen? Wie verhält sich das Konzept von Privacy zur Vertraulichkeit der Kommunikation?

Wie diese mehrdimensionale Komplexität der Schutzziele aber auch zeigt, kann Moderne Kryptographie rein technologisch nicht mehr *nur* als Mittel zur Vertraulichkeit betrachtet werden. Mit Blick auf die unterschiedlichen Schutzziele können wir auch andere, etwas subtilere Fragen des Verhältnisses von Kryptographie und Ethik analysieren: Sollte anonyme Kommunikation in Demokratien technisch möglich sein? Ist eine Authentifizierungspflicht in gewissen Situationen ethisch geboten? Kann mit Kryptographie eine Totalidentifikation des Menschen entstehen, wenn biologische Merkmale mit digitalen Zertifikaten und Signaturen verbunden werden? Unter welchen Umständen sollte eine solche Zurechenbarkeit nicht möglich sein?

All diese Fragen erfordern eine Verbindung von einer ethischen Analyse einerseits mit den technologischen Möglichkeiten Moderner Kryptographie andererseits. Kryptographische Verfahren sind dabei nämlich einem stetigen Wandel unterzogen, wie die vorangehenden Abschnitte gezeigt haben. Seit Jahrhunderten ist die Kryptographie geprägt durch das an vielen Stellen implizit beschriebene Katz-und-Maus-Spiel, bei dem

143 Gasser et al. erkennen hierbei auch Folgen für die Möglichkeiten der Überwachung: „Networked sensors and the Internet of Things are projected to grow substantially, and this has the potential to drastically change surveillance. The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access. Thus an inability to monitor an encrypted channel could be mitigated by the ability to monitor from afar a person through a different channel"; ebd., S. 3.

die *Codemaker* (Kryptographie) gegen die *Codebreaker* (Kryptoanalyse) antreten. RSA und AES sowie die meisten in der Praxis angewandten Verfahren sind lediglich *computationally secure* – das heißt, sie sind mit der *heutigen* Rechenleistung und dem *heutigen* Wissen nicht zu brechen. Das nächste Kapitel soll daher einen Ausblick auf die Zukunft der Kryptographie wagen. Insbesondere soll uns dabei die Frage beschäftigen, welche Auswirkung das Quantum Computing auf die (asymmetrische) Kryptographie hat und haben wird.

2.5 Quantum Computing und Verschlüsselung

Im Jahr 1994 veröffentlicht Peter Shor einen Algorithmus, der das wahr werden ließ, wovor sich Kryptographinnen und Kryptographen lange Zeit nur fürchten konnten: eine Methode, mit der das Faktorisierungsproblem (relevant für RSA) und das Problem des Diskreten Logarithmus (relevant für den DH-Schlüsselaustausch) in polynomieller Laufzeit gelöst werden kann.[144] Das für die asymmetrische Kryptographie bislang Beruhigende allerdings ist, dass dieser Algorithmus in der Realisierung einen sogenannten *Quantencomputer* benötigt, da an einer entscheidenden Stelle eine Quanten-Fouriertransformation durchgeführt wird. Ein Quantenrechner, der groß genug wäre, um heute verwendete RSA-Verschlüsselungen zu brechen, existiert bislang nicht.[145]

Daher findet RSA weiter breite Anwendung, ohne dass man sich zumindest kurzfristig Sorgen um die Vertraulichkeit und Authentizität von

144 Siehe Shor, „Algorithms for Quantum Computation"; einführend auch Chris J. Hoofnagle und Simson J. Garfinkel. *Law and Policy for the Quantum Age*. Cambridge: Cambridge University Press, 2022, S. 166–167 und 199–203.

145 Für diese und die folgenden Ausführungen zum Quantum Computing siehe die Standardliteratur, insbesondere LaPierre Ray. *Introduction to Quantum Computing*. Cham: Springer, 2021; Matthias Homeister. *Quantum Computing verstehen: Grundlagen – Anwendungen – Perspektiven*. 6. Aufl. Wiesbaden: Springer Vieweg, 2022; Sean Hallgren und Ulrich Vollmer. „Quantum computing". In: *Post-Quantum Cryptography*. Hrsg. von Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen. Berlin und Heidelberg: Springer, 2009, S. 15–34. Zur Post-Quanten-Kryptographie siehe Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen, Hrsg. *Post-Quantum Cryptography*. Berlin und Heidelberg: Springer, 2009; Daniel J. Bernstein. „Introduction to post-quantum cryptography". In: *Post-Quantum Cryptography*. Hrsg. von Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen. Berlin und Heidelberg: Springer, 2009, S. 1–14. Zur Einführung in das Quantum Computing im Kontext von Cyber Threats siehe Clarke und Knake, *The Fith Domain*, S. 253–264.

Kommunikation machen müsste. Zu betonen ist auch, dass für symmetrische Verfahren wie AES sowie für heute genutzte Hashfunktionen kein Algorithmus bekannt ist, der ein solch *fundamentales* Problem wie bei der asymmetrischen Kryptographie darstellen würde. Der Grover-Algorithmus ermöglicht zwar schnellere Brute-Force-Attacken auf AES, allerdings gilt AES mit einer Schlüssellänge von 256 Bit als weiterhin sicher.[146]

Trotz der aktuellen Sicherheit der bekannten asymmetrischen Verfahren gibt es mindestens drei Gründe, die dafür sprechen, die genannten Fragen auch in einer ethischen Diskussion zu berücksichtigen: (1) Dem Quantum Computing *könnte* in wenigen Jahrzehnten der Durchbruch gelingen, sodass bisher verwendete Verfahren nutzlos wären. (2) Der Prozess und die Dauer einer Migration zu einer sogenannten *Post-Quanten-Kryptographie* (engl. *Post-Quantum Cryptography*, abgekürzt PQC) ist schwer abzuschätzen. (3) Eine ganz grundsätzliche Frage praktikabler Kryptographie ist, *wie lange* die heutige Kommunikation und Information erfolgreich verschlüsselt sein soll.[147] Abschnitt 8.3 wird sich daher explizit mit ethischen Fragen zum Quantum Computing und zur Kryptographie auseinandersetzen. Um diese Fragen aber beantworten zu können, betrachten wir in diesem Kapitel zunächst die technischen Grundlagen.

Bisherige, klassische Computer arbeiten mit digitalen Schaltungen und Transistoren, die auf binäre Weise mit Nullen und Einsen Berechnungen durchführen. Dies gilt für Personal Computer (PC), mobile Endgeräte, Smartwatches, Hochleistungsrechner und IoT-Geräte. Das Quantum Computing dagegen stellt ein gänzlich neues Paradigma der Berechnung dar. Ein Quantenrechner macht sich nämlich quantenmechanische Phänomene aus der Physik zunutze, von denen ein algorithmischer Rechenvorteil gegenüber klassischen Rechnern erhofft wird. Algorithmischer Rechenvorteil bedeutet hier, dass ein Quantenalgorithmus gefunden wird, der bekanntermaßen einen Vorteil gegenüber einem klassischen Algorithmus aufweist. Der *Algorithmus von Deutsch* und der *Deutsch-Jozsa-Algo-*

146 Siehe Daniel J. Bernstein und Tanja Lange. „Post-quantum cryptography". In: *Nature* 549 (2017), S. 188–194, hier S. 189.

147 Letzteres meint vor allem Fragen zur *Vorratsdatenspeicherung* (engl. *data retention*). Siehe allgemein einführend Diffie und Landau, *Privacy on the Line*, S. 291–294. Wie in den vorherigen Abschnitten deutlich geworden ist, sind die meisten Algorithmen lediglich *computationally secure*. Ein Angriff mit unbeschränkter Rechenleistung würde daher Nachrichten, die mit solchen Algorithmen verschlüsselt wurden, brechen können.

rithmus waren die ersten Algorithmen, bei denen solche Vorteile gezeigt werden konnten.[148]

Um einen solchen Quantenvorteil zu erreichen, arbeiten Quantenrechner mit sogenannten *Qubits* – im Gegensatz zu jenen klassischen *Bits*, die entweder 0 oder 1 repräsentieren. Damit hängen wichtige quantenmechanische Phänomene zusammen, primär die sogenannte *Superposition* und die *Verschränkung*. Es würde an dieser Stelle zu weit gehen, neben den kryptographischen Aspekten auch noch jene der Quantenphysik und des Quantum Computings zu erläutern. Für weitere Ausführungen sei daher auf die umfassende Literatur verwiesen.[149] Für die Kryptographie aber ist wichtig: Sollte ein entsprechend großer und nutzbarer Quantenrechner entwickelt werden, werden die meisten der eingesetzten asymmetrischen Verschlüsselungsverfahren unbrauchbar – mit allen sozialen, ökonomischen und gesellschaftlichen Folgen. Wie weit ist die Welt davon aber entfernt?[150]

Für die Marketingabteilungen der großen Hersteller jedenfalls jagt ein Meilenstein den nächsten, der einen Quantenrechner mit immer mehr Qubits ermöglicht.[151] Allerdings spielt die Anzahl an Qubits nicht die alleinige Rolle für die Nutzbarmachung von Quantencomputern, weshalb

148 Siehe David Deutsch. „Quantum theory, the Church–Turing principle and the universal quantum computer". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), S. 97–117; sowie David Deutsch und Richard Jozsa. „Rapid solution of problems by quantum computation". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 439.1907 (1992), S. 553–558. Siehe zur Einführung auch Ray, *Introduction to Quantum Computing*, S. 149–161.

149 Für eine aktuelle, aber verständliche Einführung siehe z. B. Homeister, *Quantum Computing verstehen*, sowie umfassend Ray, *Introduction to Quantum Computing*. Auch die Unterscheidung verschiedener Ansätze im Quantum Computing, etwa des sogenannten *adiabatischen Quantum Computing*, sind hier aufgrund der gebotenen Kürze auszuklammern. Siehe im Kontext der Kryptographie einführend Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 204–206.

150 Siehe zu einer aktuelleren Einschätzung im Kontext der Kryptographie ebd., S. 203–206.

151 Für IBM war dies etwa der *IBM Eagle*, dessen Vorstellung von seinem Hersteller werbend kommentiert und tituliert wurde mit „IBM Quantum breaks the 100-qubit processor barrier". Jerry Chow, Oliver Dial und Jay Gambetta. „IBM Quantum breaks the 100-qubit processor barrier". In: *IBM Blog* (16. Nov. 2022). URL: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle (besucht am 15.04.2024). Zum Risiko des Hypes siehe auch Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 17–18.

werbende Aussagen eher von Hybris zeugen als zu einer realistischen Einschätzung der Technologie führen.[152] Eine wohlwollende Skepsis ist auch vor dem Hintergrund des ständigen Wissenszuwachses durch die Physik und der rapiden Entwicklungen in der informatischen Anwendung angebracht.[153] Denn wie in zahlreichen Bereichen der Wissenschaft gibt es auch im Bereich des Quantum Computings eine Art immanenter *Unsicherheit* – nur mit dem Unterschied, dass jene *Unsicherheit* gerade in diesem Bereich der Wissenschaft einige unangenehme und negative Folgen mit sich bringen könnte. Man kann schlichtweg nicht sagen, wann, ob oder wie dem Quantum Computing der *praktische* Durchbruch gelingen wird. Der Physiker John Preskill hat diese Situation des Quantum Computings bereits im Jahr 2018 auf den Punkt gebracht:

> While this uncertainty fuels optimism, our optimism should be tempered with caution. We may feel confident that quantum technology will have a substantial impact on society in the decades ahead, but we cannot be nearly so confident about the commercial potential of quantum technology in the near term, say the next five to ten years.[154]

Um trotzdem den Versuch einer zeitlichen Systematisierung vornehmen zu können, bietet sich das *Mosca-Theorem* an.[155] Dieses Theorem lässt sich einfach durch $X + Y > Z$ beschreiben.[156] Dabei meint X die Dauer, wie lange kryptographische Schlüssel sicher sein sollten.[157] Nachrichten können durchaus hohe Anforderungen an eine solche Dauer haben, etwa

152 Eine aktuell wichtige Thematik ist hier die Fehlerkorrektur; siehe einführend Ray, *Introduction to Quantum Computing*, S. 341–345.

153 Kritische Argumente zur generellen Realisierbarkeit von Quantencomputern finden sich beispielsweise beim israelischen Mathematiker Gil Kalai. Siehe etwa Gil Kalai. *Three Puzzles on Mathematics, Computation, and Games*. 2018. arXiv: 1801.02602v1. URL: http://arxiv.org/pdf/1801.02602v1 (besucht am 15.04.2024); sowie Gil Kalai. *The Quantum Computer Puzzle (Expanded Version)*. 2016. arXiv: 1605.00992v1. URL: http://arxiv.org/pdf/1605.00992v1 (besucht am 15.04.2024).

154 John Preskill. „Quantum Computing in the NISQ era and beyond". In: *Quantum* 2 (2018), Art. Nr. 79, S. 1. An solch einer Einschätzung hat sich bis heute wenig geändert.

155 Siehe Michele Mosca. „Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" In: *IEEE Security and Privacy* 16.5 (2018), S. 38–41.

156 Siehe ebd., S. 38.

157 Siehe ebd., S. 38. Dies ist sowohl auf das Schutzziel der Vertraulichkeit als auch auf jenes der Authentizität anwendbar.

streng vertrauliche Dokumente zur Identität von Undercover-Agenten oder zu militärischen Operationen.[158] Aber auch persönliche und intime Nachrichten möchte man sicherlich länger als nur wenige Jahre verschlüsselt wissen. Besondere Bedeutung erlangt dieser Aspekt vor dem Hintergrund der Bemühungen von Strafverfolgungsbehörden und Geheimdiensten um eine *Vorratsdatenspeicherung* (engl. *data retention*): Bereits heute kann ein substantieller Teil der Internet-Kommunikation aufgezeichnet und gespeichert werden, und man könnte spekulieren, dass dies mit der Intention geschieht, diese Kommunikation nach dem Tag X auch entschlüsseln zu können.[159]

Leider genügt es aber nicht, wenn X klein ist, zumal X primär eine Business- und Policy-Entscheidung ist.[160] Genauso bedeutend ist Y: Wie lange dauert es, quantensichere Systeme zu entwickeln und einzusetzen?[161] Vorwiegend relevant ist dabei die Migration zu einer PQC. An einer solchen PQC, die einerseits resistent gegenüber Quantenalgorithmen und andererseits auf digitalen Rechnern berechenbar ist, wird bereits seit vielen Jahren geforscht.[162] Trotzdem sind die Integration und die Migration neuer kryptographischer Verfahren in ein bestehendes System aufwendig und komplex, und eine Schätzung, wie lange es dauern könnte, gestaltet sich schwierig.

Z schließlich beschreibt die Dauer der Entwicklung eines ausreichend großen Quantenrechners, der unsere heutigen asymmetrischen Verfahren brechen kann.[163] Auch hier ist eine Schätzung kaum möglich. Im Sinne einer funktionalen Kryptographie ist Z tendenziell jedoch eher kürzer als länger einzuschätzen. Die Folgen wären technologisch und gesellschaftlich potentiell gravierend, wenn von einer falschen und zu großzügigen Dauer ausgegangen wird. Zusammenfassend ist X daher zwar

158 Als Beispiel kann hier die sowjetische Kommunikation dienen, die noch viele Jahre später im Rahmen des Venona-Projekts entschlüsselt werden sollte. Siehe Diffie und Landau, *Privacy on the Line*, S. 29–30; einführend zur Dauer auch Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 427–428.

159 Siehe im Kontext der NSA James Bamford. „The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)". In: *Wired* (12. März 2015). URL: https://www.wired.com/2012/03/ff-nsadatacenter/ (besucht am 15.04.2024); ebenso Diffie und Landau, *Privacy on the Line*, S. 292, allgemeiner siehe S. 291–294.

160 Siehe Mosca, „Cybersecurity in an Era with Quantum Computers", S. 38.

161 Siehe ebd., S. 38–39.

162 Siehe Bernstein, „Introduction to post-quantum cryptography".

163 Siehe Mosca, „Cybersecurity in an Era with Quantum Computers", S. 39.

a priori einzuschätzen und festzulegen, wird als primäre Policy-Entscheidung jedoch oft nur ungern verändert. *Y* und *Z* dagegen sind zwar bis zu einem gewissen Grad durch die entsprechende Forschung und praktische Maßnahmen zu beeinflussen, allerdings ist eine apriorische Einschätzung nicht möglich.

Neben jener bereits beschriebenen PQC, die für *Y* relevant ist, ist auch die sogenannte *Quantenkryptographie* zu nennen. Während die PQC eine quantenresistente Verschlüsselung mithilfe digitaler Rechner zum Ziel hat, nutzt die Quantenkryptographie selbst quantenmechanische Phänomene. Bedeutend ist hier vor allem der sogenannte *Quantenschlüsselaustausch* (engl. *Quantum Key Distribution*, abgekürzt QKD).[164] Erstmalig veröffentlicht wurde ein solches Verfahren 1984 von Charles H. Bennett und Gilles Brassard (daher abgekürzt mit *BB84*).[165] Benötigt wird allerdings spezielle Hardware zur Quantenkommunikation.[166] Auch hier ist damit unklar, bis wann mit einem breitflächigen und praktischen Einsatz gerechnet werden könnte.[167] Sollte es jedoch dazu kommen, wäre algorithmische *information-theoretic security* in der Kommunikation realisierbar.[168]

Die Thematik um das Quantum Computing, die PQC und die QKD ist damit nicht nur für die Physik, die Informatik und die Ingenieurwissenschaften von Interesse. Das Quantum Computing wird auch zur theoretischen Herausforderung für die Ethik, die Soziologie, die Philosophie, die Theologie und alle weiteren Humanwissenschaften werden – egal ob

164 Siehe zur Sicherheit der QKD Renato Renner. „Security of Quantum Key Distribution". Dissertation No. 16242. Zürich: ETH Zürich, 2005; einführend Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 276–293.

165 Siehe Charles H. Bennett und Gilles Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing". In: *Proceedings of the International Conference on Computers, Systems and Signal Processing. Bangalore, India*. 1984, S. 175–179; einführend auch Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 277–293.

166 Siehe zur Einführung in die Quantenkommunikation ebd., S. 257–260.

167 Siehe umfassender zur Quantenkryptographie und BB84 auch Ramona Wolf. *Quantum Key Distribution: An Introduction with Exercises*. Cham: Springer, 2021; sowie Federico Grasselli. *Quantum Cryptography: From Key Distribution to Conference Key Agreement*. Cham: Springer, 2021; im Deutschen auch Homeister, *Quantum Computing verstehen*, S. 167–189.

168 Siehe Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 257. Allerdings könnten z. B. Fehler in der Implementierung dieses Ziel auch dann noch verhindern.

und wann ein Durchbruch gelingen mag. Gerade *wegen* der Unsicherheiten von Prognosen und Einschätzungen sind die Geisteswissenschaften im Allgemeinen und die Ethik im Speziellen gefragt, einen Zugang zum Quantum Computing zu entwickeln. Einerseits geht es darum, sich auf die möglicherweise kommenden disruptiven Veränderungen vorzubereiten, sie zu analysieren und schließlich Lösungsansätze für drängende Probleme und den Einsatz von Quantencomputern zu diskutieren. Andererseits gilt es aber auch, das binäre Bild, das unsere digitale Welt über fünfzig Jahre lang in Nullen und Einsen geprägt hat, zu überdenken. Für die Kryptographie wird Abschnitt 8.3 einen solchen Zugang der Ethik entwickeln.

Kommen wir im Kontext dieser Aussichten und zum Abschluss von Teil I noch einmal auf David Kahns *The Codebreakers* zurück. Nach einer Diskussion um DES, den DH-Schlüsselaustausch und RSA schreibt er in der überarbeiteten Ausgabe seines Werkes aus dem Jahr 1996:

> The war of cryptographer against cryptanalyst has been won by the cryptographers. The only way properly encrypted messages can be read nowadays is by theft or betrayal – that is, noncryptologic means. [...] Does this mean that the story of secret writing has ended? In the long term, yes.[169]

Kahn hat ohne jeglichen Zweifel eine beeindruckende Geschichte über das *secret writing* verfasst, die sich stark am Ziel der Vertraulichkeit orientiert hat. In einem rein theoretischen Sinn hat er etwa mit Blick auf das One-Time-Pad also recht. Moderne Kryptographie ist heute jedoch mehr als bloß das. Für Kahn dürfte dies in der ersten Auflage von 1967 noch nicht klar gewesen sein, und selbst in der zweiten Auflage aus dem Jahr 1996 war die Kryptographie in weiten Teilen noch ein reines Werkzeug zum Zwecke der Vertraulichkeit.

Das Paradigma der Klassischen Kryptographie war spätestens mit dem 20. Jahrhundert beendet. Das aber, was danach kam, jene Moderne Kryptographie, steht heute erst am Anfang. Der Algorithmus von Shor, die Standardisierung von PQC und eine neue Art des Schlüsselaustausches durch die QKD zeigen ganz praktisch, dass die Diskussion um sichere Kryptographie noch einen weiten Weg vor sich hat. Auch viele

169 Kahn, *The Codebreakers*, S. 984.

andere zukünftige Themen der Kryptographie wie beispielsweise die homomorphe Kryptographie, Physical Unclonable Functions (PUF) oder Zero-Knowledge-Proofs konnten in diesem Rahmen nicht einmal ansatzweise diskutiert werden.[170]

Dieses neue Paradigma war und ist aber nicht nur technologischer Natur. Wenige Jahre nach Shannon, Diffie und Hellman erreichte die Moderne Kryptographie zunehmend auch den gesellschaftlichen Diskurs. Wenn Kommunikation schließlich immer mehr digital stattfinden sollte, dann wird sich natürlich auch jeder Einzelne und jede Einzelne fragen müssen: Wie kann meine Kommunikation sicher, vertraulich und integer sein? Der zweite Teil wird zeigen, dass diese Frage einige weitreichende gesellschaftliche Diskussionen zur Folge haben musste.

170 Der Kryptograph Yvo Desmedt meint zur Zukunft der Kryptographie sogar, dass „cryptography as a science is in its infancy." Desmedt, „What is the Future of Cryptography?", S. 113.

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.

Teil III
Kryptographie & Ethik

Kryptographie spielt eine entscheidende Rolle für das soziale Zusammenleben im 21. Jahrhundert. Diese Kryptographie ist aber nicht nur eine technologische und gesellschaftliche Angelegenheit, sondern eben auch eine *ethische Sache*. Wäre sie das nicht, könnte der Umgang mit ihr zu Beliebigkeit oder Determinismus führen. Eine ethische Normativität im Umgang mit Kryptographie wird daher nun Teil III analysieren: Welche ethischen Zugänge sind zur Kryptographie überhaupt möglich? Welche normativen Argumente sprechen für den Einsatz von Kryptographie, welche dagegen? Kann umgekehrt eine Regulierung von Kryptographie ethisch erlaubt oder sogar geboten sein? Welches *Sollen* ist im Umgang mit Kryptographie geboten?

Um diese Fragen zu beantworten, untersucht Teil III vier Themen an der Schnittstelle von Ethik und Kryptographie. In einer übergeordneten Systematik erarbeitet Kapitel 5 zunächst grundlegende ethische Zugänge zur Kryptographie. Einerseits sind hier konsequentialistische und pflichtethische Ansätze denkbar, die auf den Umgang mit Kryptographie angewandt werden können. Andererseits soll auch das Verhältnis der Menschenrechte zur Kryptographie eruiert werden. Letzteres wurde in der wissenschaftlichen Forschung bereits in Ansätzen diskutiert, insofern sowohl die Menschenrechte als auch die Moderne Kryptographie einen *globalen* Anspruch erheben. Zuletzt können aus methodologischer Perspektive auch Lessigs sogenannte *latent ambiguities* auf die Ethik angewandt werden: In konkreten Situationen sind verschiedene Interpretationen von ethischen Werten und Normen möglich. Ein neuer Kontext wie die Entwicklung der Modernen Kryptographie zwingt uns, eine Entscheidung zwischen sehr unterschiedlichen normativen Aussagen zu treffen.

Kapitel 6 analysiert Zielkonflikte und (Schein-)Dichotomien im Kontext der Kryptographie. Solche argumentativen Konflikte treten im Diskurs um den richtigen Umgang mit Kryptographie immer wieder auf. Ihnen ist gemein, dass sie oftmals eine konsequentialistische Programmatik verfolgen, die sich an zwei unterschiedlichen Konsequenzen der Verschlüsselungstechnologien orientiert. Zunächst ist dies sichtbar am Argument der *Kryptographie als Dual-Use-Technologie*, dem zufolge Ver-

schlüsselung sowohl für zivile als auch für militärische Zwecke genutzt werden kann. Im Anschluss zeigt sich auch eine scheinbare Dichotomie von *Privacy vs. Sicherheit*, nach der wir entscheiden müssen, ob wir mehr Privacy oder mehr Sicherheit wollen. Zuletzt ist die scheinbare Dichotomie aus *Überwachung vs. Kryptographie* zu untersuchen, laut der Verschlüsselung die Überwachung verhindern wird. Mit ethischen wie auch technologischen Begründungen können alle drei Argumente gegen die Kryptographie widerlegt werden.

Kapitel 7 beschäftigt sich schließlich mit drei Spezialthemen der Ethik der Kryptographie: Transparenz, Gleichheit und Identität. Alle drei gehen von der Modernen Kryptographie aus, die einen wissenschaftlichen, globalen und für alle zugänglichen Charakter aufweist.[1] Dazu sind zunächst Missverständnisse zum Verhältnis von Transparenz und Verschlüsselung zu klären. Denn obschon Kryptographie das Ziel der Geheimhaltung respektive Vertraulichkeit verfolgt, ist ihr Verhältnis zur Idee der allgemeinen, gesellschaftlichen und politischen Transparenz weitaus komplexer. Darauf aufbauend wird das Konzept der sogenannten *egalitären Kryptographie* entwickelt: einer Kryptographie, die *von allen* auch tatsächlich genutzt wird. Bisherige Regulierungsversuche, so das vorgestellte Argument, widersprechen jedoch dieser Idee. Zuletzt befasst sich das Kapitel mit einem Bereich, der das Schutzziel der Authentizität inkludiert: Identifikation mithilfe von Kryptographie. Dabei sind die Bedeutung und die Gefahren von Identifikationsmechanismen im Kontext der Modernen Kryptographie zu erarbeiten.

Kapitel 8 ermöglicht schließlich eine Synthese aus allen bisherigen Teilen, bei der aktuelle Anwendungsfragen diskutiert werden. Dabei sollen noch einmal die technologischen Grundlagen der Kryptographie aus Teil I sowie die gesellschaftlichen Rahmenbedingungen aus Teil II aufgegriffen werden. Zunächst ist das sogenannte *Client-Side-Scanning* (CSS) zu analysieren. Entscheidende Gründe sprechen denn dafür, dass das CSS aus ethischer Perspektive strikt abzulehnen ist. Anschließend befasst sich das Kapitel mit der Möglichkeit der Regulierung über Intermediäre. Auch wenn dies eine weitverbreitete Art der Steuerung von Kryptographie ist, treten dabei ethische Probleme auf. Zuletzt soll nach der Zukunft einer (Ethik der) Kryptographie gefragt werden. Teil I hat bereits deutlich ge-

1 Siehe Katz und Lindell, *Introduction to Modern Cryptography*, S. 3, sowie Adams, *Introduction to Privacy Enhancing Technologies*, S. 242; zur Diskussion auch Kapitel 2.

macht, dass die Entwicklung von Verschlüsselungstechnologien bislang nicht an ihr Ende gekommen ist. Auch die kommenden Herausforderungen und Unsicherheiten sollen daher in diesem letzten Abschnitt mit Blick auf das Quantum Computing analysiert werden.

5 Ethische Zugänge zur Kryptographie

> Advances in technology will not permit the maintenance of the status quo, as far as privacy is concerned. The status quo is unstable. If we do nothing, new technologies will give the government new automatic surveillance capabilities that Stalin could never have dreamed of. The only way to hold the line on privacy in the information age is strong cryptography.
>
> – Phil Zimmermann[1]

Kapitel 5 soll einerseits eine Einführung in die Ethik selbst sein. Eine Ethik der Kryptographie kann nur interdisziplinär sein, wenn sie sowohl für die Ethik als auch für die Natur- und Ingenieurwissenschaften zugänglich ist. Ein solcher Zugang erfordert, dass manche Teile der Arbeit für Personen von einer der beiden Professionen als selbstverständlich empfunden werden. Teil I war ein solcher Abschnitt, der für manche aus dem Bereich der Kryptographie allzu bekannt gewesen sein dürfte. Kapitel 5 ist hingegen der Abschnitt, in dem Forschende aus der Ethik viel Bekanntes erkennen werden. Eine solche gegenseitige Offenheit ist Voraussetzung für die Zugänglichkeit einer Ethik der Kryptographie.

Andererseits ist dieses Kapitel aber auch weit mehr als nur eine Einführung in die Ethik. Es geht darum, einen *strukturierten* Zugang zu einer Ethik der Kryptographie zu entwickeln.[2] Diese Struktur ermöglicht es, verschiedene Argumente für oder gegen eine freie und zugängliche Kryptographie systematisch in eine ethische Argumentation einzuordnen. Dazu werden Beispiele von Fragen und Argumenten identifiziert, die so oder so ähnlich seit vielen Jahren normativ diskutiert, jedoch nur selten anhand der ihnen zugrundeliegenden, impliziten Ethik systematisiert werden. Diese Argumente und Fragen erkennen und anschließend methodisch einordnen zu können, ist Ziel von Kapitel 5 und Grundlage für die nachfolgenden Kapitel.

---

1 Zimmermann, *Why I Wrote PGP*.

2 Bislang ist das dedizierte Verhältnis von Ethik und Kryptographie in der Forschung wenig beachtet worden. Eine positive Ausnahme aus dem Bereich der Kryptographie ist hier Phillip Rogaway. *The Moral Character of Cryptographic Work*. 2015. Cryptology ePrint Archive: 2015/1162. URL: https://eprint.iacr.org/2015/1162 (besucht am 15.04.2024).

Zunächst wird sich Abschnitt 5.1 mit konsequentialistischen und pflichtethischen Ansätzen auseinandersetzten, welche die Philosophiegeschichte und Ethik seit Langem prägen. Anschließend untersucht Abschnitt 5.2 die Verbindung von Menschenrechten und Kryptographie, da gerade hier bereits einiges an ethischer Reflexion über den Einsatz von Verschlüsselungstechnologien stattgefunden hat. Zuletzt diskutiert Abschnitt 5.3 ein Thema aus Lessigs *Code: Version 2.0* – die sogenannten *latent ambiguities*. Methodisch wird dieser letzte Abschnitt zeigen, dass die Herausforderung einer Ethik der Kryptographie nicht nur in einer systematischen Ethik liegt, sondern vor allem in der Verbindung mit neuartigen technologischen Möglichkeiten, Kontexten und Notwendigkeiten.

5.1 Konsequentialistische und pflichtethische Ansätze

In der *normativen Ethik* gibt es nicht die *eine* Theorie schlechthin, die nur noch auf den konkreten Fall der Kryptographie angewandt werden müsste.[3] Vielmehr haben über zweitausend Jahre Ethikdiskurs gezeigt, dass die Vorstellung über das *Gute* und das *Schlechte* zu unterschiedlichen normativen Theorien und Antworten führt. Man sollte dies aber nicht als kulturellen Relativismus oder ethischen Nihilismus abtun. Im Folgenden gilt für die Diskussion vielmehr die Maxime, das bestmögliche ethische Argument auf der Basis von Vernunft und Logik zu eruieren.[4] Für einen solchen Versuch ist es hilfreich, unterschiedliche ethische Theorien auf den Anwendungsfall der Kryptographie zu beziehen. Kann gezeigt werden, dass diese unterschiedlichen Theorien ähnliche Antworten im Kontext der Kryptographie liefern, gewinnt eine solche Ethik der Kryptographie an Überzeugungskraft. Führen diese Theorien hingegen zu unterschiedlichen Schlüssen, kann auch dadurch ein Erkenntnisgewinn entstehen, indem das überzeugendere Argument ermittelt werden kann.

Zwei dieser normativen ethischen Theorien, die im Laufe der jüngeren Philosophiegeschichte am einflussreichsten waren, werden im Fol-

3 Siehe einführend zur normativen Ethik z. B. Jonathan Wolff. *An Introduction to Moral Philosophy*. New York und London: W. W. Norton & Company, 2018, S. 5–6; sowie Herlinde Pauer-Studer. *Einführung in die Ethik*. 3. Aufl. Wien: Facultas, 2020, S. 14–21.

4 Auch der Vernunftbegriff bedürfte hier bereits einer vertiefenden Auseinandersetzung. Im Sinne des Fokus auf eine Ethik der Kryptographie kann er jedoch nicht näher aus metaphysischer wie auch metaethischer Perspektive beleuchtet werden.

genden vertiefter diskutiert.[5] Einerseits ist dies der *Konsequentialsmus*, der als Maßgabe das richtige und gute Handeln an den Folgen des Handelns orientiert (oftmals in der Form des *Utilitarismus*), andererseits die *Pflichtethik* (oder *Deontologie*), bei der explizit nicht die Folgen des Handelns entscheidend sind, sondern ob die Handlung aufgrund einer Pflicht geboten ist. Weitere Formen einer normativen Ethik sind zudem die auf Aristoteles zurückzuführende *Tugendethik*, bei der der Fokus des Handelns stark auf das Individuum und einen guten Charakter gelegt wird, sowie die *Diskursethik* Apels und Habermas', bei der die ethische Legitimität einer Norm durch einen Diskurs und die Akzeptanz seitens der Diskursteilnehmerinnen und -teilnehmer ermittelt werden soll.[6] Auf die beiden letztgenannten Theorien wird jedoch im Rahmen der folgenden Grundlegung nicht näher eingegangen, lässt doch bereits die Begründung einer Ethik *der Kryptographie* einen starken thematischen Fokus erkennen, weshalb der Raum zur Diskussion weiterer ethischer Theorien beschränkt werden muss. Diese bewusste Lücke der Forschung kann und soll durch spätere Arbeiten allerdings geschlossen werden.[7]

Diese Arbeit versteht sich in erster Linie als eine normative Untersuchung. Allerdings kann es hilfreich sein, an vereinzelten Stellen auch die anderen Bereiche der Ethik zu diskutieren. Denn was überhaupt meint *gut* und *schlecht*, *richtig* und *falsch*? Der Teilbereich der Ethik, der sich mit solchen grundsätzlichen Fragen auseinandersetzt, nennt sich *Metaethik*.[8] In der Metaethik werden daher auch keine bewertenden Aussagen über Handlungen getroffen, diese fallen in den Bereich der normativen Ethik.

5 Siehe zur Einführung in die Theorien und zum Folgenden Dagmar Fenner. *Ethik: Wie soll ich handeln?*. 2. Aufl. Tübingen: Narr Francke Attempto Verlag, 2020, S. 161–188, zur Diskursethik auch S. 146–154; zudem Michael Quante. *Einführung in die Allgemeine Ethik*. 2. Aufl. Darmstadt: WBG, 2006, S. 126–142; einführend Friedo Ricken. *Allgemeine Ethik*. 4. Aufl. Stuttgart: Verlag W. Kohlhammer, 2003, S. 271–299. Oftmals wird in der Literatur der *Utilitarismus* als bekannteste Form des Konsequentialismus diskutiert. Dieses Verhältnis wird weiter unten diskutiert.

6 Siehe zur Tugendethik im Speziellen einführend Fenner, *Ethik*, S. 175–179, sowie Wolff, *An Introduction to Moral Philosophy*, S. 200–31; zur Diskursethik einführend Fenner, *Ethik*, S. 146–154, sowie Pauer-Studer, *Einführung in die Ethik*, S. 57–63.

7 Selbiges gilt etwa auch für einen Anschluss einer Ethik der Kryptographie an die *christliche Soziallehre*.

8 Siehe zur Einführung in die Metaethik Wolff, *An Introduction to Moral Philosophy*, S. 5; sowie John Deigh. *An Introduction to Ethics*. Cambridge: Cambridge University Press, 2010, S. 196–201; außerdem Annemarie Pieper. *Einführung in die Ethik*. 2. Aufl. Tübingen: Francke Verlag, 1991, S. 78–83.

Dennoch sind normative Ethik und Metaethik nicht völlig separiert: Ohne eine begriffliche oder methodologische Auseinandersetzung ist auch die Frage nach dem konkret *moralisch richtigen* Handeln ohne Fundament. Solche metaethischen Fragestellungen treten etwa in Abschnitt 5.3 auf.

Der dritte Bereich der Ethik als Wissenschaft ist üblicherweise die *deskriptive Ethik*.[9] Diese hat ebenso keine normativen Bewertungen zum Ziel, sondern ein rein empirisches Untersuchen der Meinungen über Moral respektive Moralität.[10] Die deskriptive Ethik ist daher eng mit den empirischen Wissenschaften und der Soziologie verknüpft, die die Einstellungen der Menschen in unterschiedlichen Gruppen, Regionen und Kulturen auf der Welt untersuchen will. Teil II hat bereits qualitativ analysieren können, welche Welt- und Wertvorstellungen beispielsweise Strömungen wie die Cypherpunks vertreten.[11]

Die normative Ethik, die Metaethik und die deskriptive Ethik bilden üblicherweise die philosophische Ethik als wissenschaftliche Disziplin.[12] Mit der fortschreitenden Spezialisierung der Forschung, einer notwendigen Interdisziplinarität in bestimmten Fragen alltäglichen Lebens und einer generellen Technologisierung des gesellschaftlichen Zusammenlebens entwickelte sich in den vergangenen Jahren aber noch ein weiterer Bereich: die *angewandte Ethik* respektive *Bereichsethik*.[13] Einerseits ist im Kontext der Ethik der Kryptographie für die Bedeutung einer sol-

9 Siehe zur Einführung in die deskriptive Ethik Otfried Höffe. *Ethik: Eine Einführung*. München: Verlag C. H. Beck, 2013, S. 25–26; sowie Quante, *Einführung in die Allgemeine Ethik*, S. 16–17.

10 Begrifflich ist im Folgenden die philosophisch-wissenschaftliche Auseinandersetzung mit *Moralität* als *Ethik* definiert; siehe dazu Deigh, *An Introduction to Ethics*, S. 8. Diese Auseinandersetzung kann normativer, aber auch deskriptiver Natur sein. Teilweise werden in der Literatur die Begriffe *ethisch* und *moralisch* synonym verwendet, so beispielsweise bei Wolff, *An Introduction to Moral Philosophy*, S. 7. Eine begriffliche Präzisierung ist allerdings hilfreich, um den Untersuchungsgegenstand der Ethik (der die Moral ist) von der Ethik als wissenschaftlicher Disziplin differenzieren zu können. Ob für die deskriptive Ethik der Begriff *Ethik* insofern überhaupt angemessen ist, ist nicht Teil der Diskussion. Siehe zur kritischen Auseinandersetzung etwa Quante, *Einführung in die Allgemeine Ethik*, S. 17.

11 Eine Quantifizierung der Meinungen und Vorstellungen über den Einsatz von Kryptographie ist angesichts der normativen Ausrichtung der folgenden Kapitel weder möglich noch intendiert, wäre aber von empirischer Relevanz. Eine solche soziologische Forschung könnte daher an die bisherigen Analysen anschließen.

12 Siehe etwa ebd., S. 16.

13 Siehe zur Einführung in die angewandte Ethik Wolff, *An Introduction to Moral Philosophy*, S. 6–7, sowie Fenner, *Ethik*, S. 21–22; umfassender auch Dagmar Fenner.

chen angewandten Ethik zu argumentieren, andererseits soll aber auch ihr methodologisches Fundament geklärt werden. Für eine Arbeitsdefinition orientieren sich die folgenden Kapitel daher an der – vereinfachten, aber hilfreichen – Annahme, dass die angewandte Ethik zum Ziel hat, ethische Normativität auf lebensnahe Situationen anzuwenden, oftmals im interdisziplinären Austausch mit angrenzenden Wissenschaften wie etwa der Medizin, Biologie, Informatik und anderen Forschungsfeldern.[14] Die angewandte Ethik ist in dieser Definition eine Teildisziplin der normativen Ethik.[15]

Offen bleibt dann aber, wie das genauere und wechselseitige Verhältnis von normativer Ethik und Situationsbezug der angewandten Ethik exakt zu bestimmen sei.[16] Zwei scheinbar konträre Modelle bieten sich hier an: ein *Top-down*-Modell und ein *Bottom-up*-Modell.[17] Im Top-down-Modell wird zunächst von universellen Normen und Prinzipien ausgegangen, deren Erkenntnisse anschließend auf den konkreten Fall angewandt werden.[18] Es handelt sich um einen deduktiven Prozess, der bei den übergeordneten Prinzipien beginnt.[19] In einem Top-down-Modell ist die angewandte Ethik daher stark unter die normative Ethik subsumiert. Das

Einführung in die Angewandte Ethik. Tübingen: Narr Francke Attempto Verlag, 2010, und Höffe, *Ethik*, S. 106–116.

14 Diese Definition orientiert sich teilweise an Fenner, *Ethik*, S. 21–22.

15 Siehe ebd., S. 22.

16 Siehe zu einer Diskussion um dieses Verhältnis auch Pauer-Studer, *Einführung in die Ethik*, S. 27–29.

17 Siehe Dagmar Fenner. „Angewandte Ethik zwischen Theorie und Praxis. Systematische Reflexionen zum Theorie-Praxis-Verhältnis der jungen Disziplin". In: *Zeitschrift für philosophische Forschung* 63.1 (2009), S. 99–121, S. 100–101, bzw. Fenner, *Einführung in die Angewandte Ethik*, S. 10–12. So wird dies etwa im Bereich des maschinellen Lernens und der Artificial Intelligence diskutiert; siehe Virginia Dignum. *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*. Cham: Springer, 2019. Aber auch im Kontext der Medienethik wird diese Modellunterscheidung vorgenommen; siehe Alexander Filipović. „Angewandte Ethik: Grundbegriffe der Kommunikations- und Medienethik (Teil 2)". In: *Soziale Kommunikation im Wandel: 50 Jahre Medienethik und Kommunikation in Kirche und Gesellschaft*. Hrsg. von Klaus-Dieter Altmeppen, Alexander Filipović und Renate Hackel-de Latour. Baden-Baden: Nomos, 2017, S. 122–128; im Menschenrechtskontext auch James Griffin. *On Human Rights*. Oxford und New York: Oxford University Press, 2008, S. 29–30.

18 Siehe Fenner, „Angewandte Ethik zwischen Theorie und Praxis", S. 100–101; diskutiert auch in Filipović, „Angewandte Ethik", S. 123–124.

19 Siehe Fenner, „Angewandte Ethik zwischen Theorie und Praxis", S. 101.

Bottom-up-Modell hingegen kehrt dieses Verhältnis um: Hier wird von konkreten Situationen und Erfahrungen ausgegangen, woraus Prinzipien und Normen für ähnliche Fälle induziert werden sollen.[20] Dadurch lässt das Bottom-up-Modell Erkenntnisfindung beruhend auf der Situation zu, wodurch es eher als eigenständiger und expliziter Teil der normativen Ethik verstanden werden kann.

Im Rahmen dieser Arbeit soll ein pragmatischer Ansatz verfolgt werden, der sich zwar der Modelle bewusst ist, sich gleichzeitig aber nicht ausschließlich für eines der beiden entscheidet. Ein solcher methodischer Ansatz ist kritisierbar – und trotzdem ist er im Rahmen einer Ethik *der Kryptographie* hilfreich. Begründet ist dies damit, dass der Bereich der Kryptographie zwangsläufig einen Realitätsbezug erfordert. Eine Ethik der Kryptographie kann nicht von künstlichen Situationen, Lösungen oder Dilemmata sprechen, die *faktisch* gar nicht zur Disposition stehen *können*. Um dazu nur ein Beispiel aus dem Kontext der Ende-zu-Ende-Verschlüsselung zu nennen: Man könnte zwar eine Kryptographie wollen, die einerseits den unbescholtenen Individuen Privatsphäre gewährleistet und es andererseits erlaubt, das Handeln der Kriminellen aufzudecken. Wir könnten dabei argumentieren, dass eine Kryptographie für die *gute* Kommunikation ethisch geboten und für die *böse* Kommunikation ethisch abzulehnen wäre. Solch eine differenzierte Kryptographie kann und wird es allerdings *per definitionem* nicht geben. Bei einer Unterscheidung anhand des Inhalts der Kommunikation wird unweigerlich das Schutzziel der kryptographischen Vertraulichkeit verletzt. Diese Argumentation ist in sich widersprüchlich und im wörtlichen Sinne *realitätsfern*.[21] Die Realität der Kryptographie muss daher als beschränkender *Rahmen* ethischer Optionen gelten.

Gleichzeitig muss es keineswegs *innerhalb* dieses Rahmens zu Beliebigkeit, Relativismus oder gar Nihilismus kommen. Um beim bisherigen Beispiel zu bleiben: Zwar ist es aufgrund der Realität der Kryptographie unmöglich, nur den *guten* Individuen Vertraulichkeit zu gewähren, nicht aber den *bösen* Kriminellen. Doch das bedeutet nicht, dass wir ausgehend von dieser Situation nicht ethisch, objektiv und vernunftbasiert über das richtige Handeln nachdenken könnten. Dabei stellen sich nämlich etwa folgende Fragen: Wie gehen wir als Gesellschaft mit dieser Realität um?

20 Siehe Fenner, „Angewandte Ethik zwischen Theorie und Praxis", S. 101.

21 Abschnitt 8.1 wird näher auf dieses Beispiel eingehen, wobei insbesondere das sogenannte Client-Side-Scanning (CSS) analysiert wird.

Sollen wir das Prinzip der Ende-zu-Ende-Verschlüsselung aufgegeben? Sollen sowohl unbescholtene Personen als auch Kriminelle überwacht und abgehört werden? Oder spricht sich die Ethik für eine freie und zugängliche Kryptographie aus, auch wenn dies dann für Kriminelle gleichermaßen gilt?

Sowohl die Argumentation als auch die Beantwortung dieser Fragen hängen von der zugrundeliegenden normativen Theorie ab – ob sie nun konsequentialistisch, pflichtethisch oder menschenrechtsbasiert ist.[22] Wir müssen uns zu diesem Zeitpunkt jedoch nicht strikt für eine der genannten Theorien entscheiden. Für eine möglichst breite Akzeptanz einer Ethik der Kryptographie lohnt es sich, eine solche Offenheit der Argumentation beizubehalten. Um das Zusammenwirken von Ethik und Kryptographie zu systematisieren, wird im Folgenden zunächst in den Konsequentialismus und die Pflichtethik eingeführt. Der darauf folgende Abschnitt befasst sich explizit mit menschenrechtsbasierten Argumentationen.

Konsequentialismus

Gerade im Bereich der Technikethik und Technikphilosophie bietet sich zunächst eine konsequentialistische Argumentation im Sinne einer sogenannten *Technikfolgenabschätzung* an.[23] Bei einer solchen Technikfolgenabschätzung können die Auswirkungen, Risiken und Gefahren von Technik und Technologie systematisch untersucht und bewertet werden. Diese Untersuchung ist damit oftmals fokussiert auf den *Outcome* – die Folgen. Der Konsequentialismus ist in diesem Kontext sehr breit definiert. Dies sollte aber nicht darüber hinwegtäuschen, dass über die Jahre eine Vielzahl an unterschiedlichen Ausprägungen des Konsequentialismus entwickelt wurden.

22 Natürlich können auch die Menschenrechte in enger Beziehung zu konsequentialistischen und/oder pflichtethischen Argumentationen stehen.

23 Siehe zur Einführung in die Technikfolgenabschätzung und zum Folgenden Marc Dusseldorp. „Technikfolgenabschätzung“. In: *Handbuch Technikethik*. Hrsg. von Armin Grunwald und Rafaela Hillerbrand. 2. Auflage. Stuttgart: J. B. Metzler, 2021, S. 442–446; zur theoretischen Einführung zum *Technology Assessment* siehe Riebe, *Technology Assessment of Dual-Use ICTs*, S. 23–28, und Arie Rip. „Technology Assessment“. In: *International Encyclopedia of the Social & Behavioral Sciences*. Hrsg. von James D. Wright. 2. Aufl. Bd. 24. Amsterdam: Elsevier, 2015, S. 125–128.

Die bekannteste und verbreitetste Strömung des Konsequentialismus ist der *Utilitarismus*, der auf den *Nutzen* (lat. *utilis* für *nützlich*) einer Handlung zielt und historisch auf Jeremy Bentham (1748–1832) und John Stuart Mill (1806–1873) zurückgeht.[24] Bereits an diesen beiden Vertretern zeigt sich, dass auch der Utilitarismus keineswegs immer die gleiche Agenda verfolgt. So ist zunächst zu fragen: Was überhaupt ist eine *gute Folge*? Was ist *Nutzen*? Und vor allem *für wen*? Für Bentham stand das größte Glück der meisten Menschen im Mittelpunkt seiner Ethik, womit er eine Art rechnerischer Wägbarkeit von Nutzen vertrat.[25] Mill fokussierte seinen Utilitarismus stärker auf die Qualität der Freuden, wobei manche wertvoller seien als andere.[26] Über diese zwei bekannten Vertreter hinaus hat sich der Utilitarismus seither in eine „beinahe verwirrende Zahl von Positionen und Unterpositionen ausdifferenziert“[27].

Im ersten Schritt beschränken wir uns jedoch im Rahmen einer Technikfolgenabschätzung auf die Anwendbarkeit eines Konsequentialismus und befassen uns weniger mit einem normativ konnotierten Nutzen respektive dessen Werttheorie.[28] Die Anwendbarkeit eines solchen Konsequentialismus auf die Kryptographie scheint auf den ersten Blick gegeben: Kryptographie kann an dem gemessen werden, was aus ihrer Anwendung folgt. Unterschiedliche Konsequenzen sind zu erwarten, wenn unterschiedlich mit Kryptographie umgegangen wird. Im zweiten Schritt können wir dann allerdings normativ im Sinne eines Utilitarismus auch fragen, welcher *Nutzen* (oder auch *Schaden*) entsteht. Wenn wir uns zur Vereinfachung des Beispiels zunächst auf das Schutzziel der Vertraulichkeit beschränken, könnten wir zum Beispiel argumentieren, dass private Kommunikation für das Individuum eine positive Erfahrung ist oder so-

24 Siehe einführend zu Bentham, Mill und der utilitaristischen Ethik Wolff, *An Introduction to Moral Philosophy*, S. 3, 125–143. Erste Ansätze zum Utilitarismus gibt es bereits bei Hobbes und Hume; siehe Peter Fischer. *Einführung in die Ethik*. München: Wilhelm Fink Verlag, 2003, S. 123.

25 Siehe Pauer-Studer, *Einführung in die Ethik*, S. 70–71.

26 Siehe ebd., S. 72–74.

27 Höffe, *Ethik*, S. 61. Man könnte annehmen, dass der Utilitarismus oftmals vorwiegend eine reine Individualethik ist. Dies lässt sich aber historisch anhand der Schriften von Bentham nicht bestätigen, insofern hier auch von Regierung und Gesetzgebung gesprochen wird. Siehe dazu Fischer, *Einführung in die Ethik*, S. 123.

28 Für den klassischen Utilitarismus ist nach Fischer die Werttheorie bzw. der Hedonismus eines von vier Merkmalen neben Konsequentialismus, Kosten-Nutzen-Kalkül sowie Allgemeinheit; siehe ebd., S. 123–124.

gar eine Art Freude bereitet. Der Mensch zieht damit Nutzen aus der Möglichkeit vertraulicher Kommunikation und bevorzugt daher auch die Anwendung der Kryptographie. Umgekehrt würde dies bedeuten, dass dann, wenn in einem autokratischen Regime vertrauliche und kryptographisch geschützte Kommunikation unterbunden wird, dies für die Möglichkeit der Privatsphäre des Einzelnen negative Folgen hätte. Im Sinne dieses Konsequentialismus respektive Utilitarismus wäre daher ein solches Handeln ethisch abzulehnen.

Allerdings könnten wir hier auch anders argumentieren. Eine Gesellschaft hätte vielleicht das begründete Interesse, private Kommunikation zu beschränken – mit der Argumentation, dass unter dem Deckmantel der vertraulichen Kommunikation Leid erzeugt wird (etwa durch die scheinbar nicht mehr mögliche Verfolgung von Straftaten). Vorstellbar ist, dass dieses Argument im Rahmen der Terrorismusbekämpfung oder der nationalen Sicherheit zum Zuge kommt. Das Glück oder die Freude der Gesellschaft wird durch den allgegenwärtigen Einsatz von Kryptographie minimiert, weshalb der Einsatz von Kryptographie reguliert und beschränkt werden sollte. In diesem Fall handelt es sich um das Argument des sogenannten *Going-Dark-Problems*, dessen Überzeugungskraft in Kapitel 6 näher analysiert wird. Nach diesem Argument hätten Strafverfolgungsbehörden und das Justizsystem keine oder nur sehr beschränkte Möglichkeiten, auf die Kommunikation von Verdächtigen oder Beschuldigten zuzugreifen, wenn Kryptographie ubiquitär genutzt wird.[29]

Das bisherige Beispiel bezieht sich auf das Schutzziel der Vertraulichkeit. Ein anderes, gesellschaftlich und ethisch relevantes Schutzziel ist das der Authentizität.[30] Kryptographische Verfahren zur Authentifizierung sind genauso allgegenwärtig wie solche zur Vertraulichkeit. Wenn Authentizität nun nicht mehr nur technisch und digital betrachtet, sondern mit der Möglichkeit der (menschlichen) Identifikation verbunden wird, ergeben sich zahlreiche, ethische Fragen. Eine konsequentialistische Argumentation ermöglicht auch auf diese Fragen sehr unterschiedliche Antworten.

---

29 Siehe einführend Gasser u. a., *Don't Panic*; John Mylan Traylor. „Shedding Light on the 'Going Dark' Problem and the Encryption Debate". In: *University of Michigan Journal of Law Reform* 50.489 (2016); sowie Bert-Jaap Koops und Eleni Kosta. „Looking for Some Light Through the Lens of 'Cryptowar' History: Policy Options for Law Enforcement Authorities Against ‚Going Dark'". In: *Computer Law & Security Review* 34 (2018), S. 890–900.

30 Aus kryptographischer Perspektive siehe Abschnitt 2.4.

Zunächst können wir hier wieder den Fall betrachten, in dem Authentifikation etwas *Gutes* ist, weil der Nutzen im utilitaristischen Sinne gegeben ist. Wir möchten etwa, dass unsere täglichen Nachrichten über Messengerdienste auch wirklich die Personen erreichen, an die sie adressiert sind. Ebenso wollen wir wissen, von wem die Nachrichten stammen, die wir erhalten. Und beim Online-Banking möchten wir, dass die Kommunikation wirklich mit unserer eigenen Bank stattfindet – und nicht mit einer bösartigen Partei, die die Website sehr gut fälschen konnte. Falls wir keine Authentifizierungsmöglichkeiten hätten und all dies nicht mehr möglich wäre, wären negative Konsequenzen zu befürchten. In all diesen Fällen verlassen wir uns auf kryptographische Protokolle.[31] Wenn wir von solch einer technischen Authentifizierung ausgehen, ist dieses Argument zweifelsfrei stimmig, und kaum jemand würde auf die Möglichkeit der Authentizität im Internet verzichten wollen.

In Verbindung mit menschlicher Identifikation wird eine konsequentialistische Argumentation allerdings komplexer. Zunächst können wir auch hier wieder eine Position einnehmen, in der wir für den Nutzen einer solchen Technologie argumentieren. An vielen Stellen des heutigen Lebens ist eine Identifikation gefordert, zum Beispiel bei der Eröffnung eines neuen Kontos oder bei der Einreise in ein Land. Dabei ist es erforderlich, den Personalausweis oder Reisepass zur Verifikation und Authentifizierung der Person vorzuzeigen. Wird ein solches Dokument per E-Mail oder über andere, unsichere Kommunikationskanäle gesendet, besteht die Gefahr, dass böswillige Parteien die Daten ausspähen. Eine sogenannte *digitale ID* oder *e-ID* könnte genau dies verhindern, indem sie einen persönlichen Identitätsnachweis auf der Basis kryptographischer Verfahren ermöglicht.[32] Zunächst scheint dies nicht nur den Komfort der Nutzerinnen und Nutzer zu erhöhen, sondern auch die Sicherheit des Systems.

---

31 Dabei handelt es sich hier insbesondere um digitale Signaturen auf der Basis asymmetrischer Kryptographie; siehe Abschnitt 2.3 und Abschnitt 2.4.

32 Siehe einführend zu digitalen IDs etwa Blaž Podgorelec, Lukas Alber und Thomas Zefferer. „What is a (digital) identity wallet? A systematic literature review". In: *IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*. 2022, S. 809–818. Ein Beispiel für eine solche regulatorische Gesetzgebung wäre etwa die eIDAS-Verordnung der EU; siehe Europäische Union. *Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG*. Amtsblatt der Europäischen Union L 257/73. 23. Juli 2014. Siehe zum Vorschlag einer Überarbeitung auch Europäische Kommission. *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung*

Dennoch sind auch hier wieder andere Argumentationen möglich. Wenn eine Authentifizierung *zu einfach* wird, könnte die Folge sein, dass eine Identifizierung allgegenwärtig wird.[33] Wenn jemand ein Eis in der Eisdiele bezahlt, sich in einen Social-Media-Account einloggen möchte oder online eine Suchanfrage stellt, so ist in all diesen Fällen eine Identifikation per Ausweis nicht notwendig. Genau das aber könnte auf einfachem Weg implementiert und gefordert werden. Wird eine kryptographisch unterstützte Identifikation sogar mit biometrischen Merkmalen verbunden, ist es nahezu unmöglich, dieser Identifikationspflicht zu entkommen. In der Konsequenz würde es sich daher um das Gegenteil von Anonymität und Pseudonymität handeln. Die Folge wäre eine Gesellschaft, in der die Möglichkeit der Nachverfolgbarkeit und Identifizierung ubiquitär wäre.

Der Utilitarist Bentham hat sich zumindest indirekt mit ähnlichen Fragen auseinandergesetzt. Auf ihn geht eine der bekanntesten Ideen einer Gefängnisarchitektur zurück, die oftmals im Zusammenhang mit Überwachung und Kontrolle zitiert wird: das *Panopticon*.[34] Die Idee dabei ist, dass von einem Punkt in der Mitte des Gefängnisses die Insassinnen und Insassen dauerhaft überwacht werden *können*, durch die Lichtverhältnisse der Wärter jedoch nicht sichtbar ist. In der Konsequenz kann eine Insassin oder ein Insasse nie wissen, ob sie oder er in diesem Moment überwacht wird oder nicht.[35] Breitere Bekanntheit erlangte diese Idee später durch Michael Foucault.[36] Die heute oft gezogene Analogie ist, dass in einer überwachten Gesellschaft (etwa mit allgegenwärtigen Kameras) niemand je sicher sein kann, nicht überwacht zu werden. Auch wenn die Analogie eines Gefängnisses auf das gesamtgesellschaftliche Leben nicht

---

der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität. COM(2021) 281 final. 3. Juni 2021. Weiterführend auch Amir Sharif u. a. „The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes". In: *Applied Sciences* 12.24 (2022), Art. Nr. 12679. Lessig setzt sich ebenso intensiv mit der Identifizierung auseinander; siehe Lessig, *Code*, S. 45–54.

33 Siehe ebd., S. 54.

34 Siehe einführend David Lyon. *The Electronic Eye: The Rise of Surveillance Society*. Cambridge: Polity Press, 1994, S. 57–79.

35 Siehe ebd., S. 62–64.

36 Siehe Michael Foucault. *Discipline and Punish: The Birth of the Prison*. 2. Aufl. New York: Vintage Books, 1995; einführend dazu auch Lyon, *The Electronic Eye*, S. 62–67, sowie David Lyon. *Surveillance society: Monitoring everyday life*. Buckingham und Philadelphia: Open University Press, 2005, S. 114–118.

unkritisch zu sehen ist, zeigt sich hier doch eindrücklich, welche unterschiedlichen und konträren Argumente des Utilitarismus möglich sind.[37]

Die ethische Bewertung anhand des Konsequentialismus wird zudem durch einen weiteren Aspekt verkompliziert: In beiden Fällen – Beschränkung von vertraulicher Kommunikation sowie digitaler Identifikationsmöglichkeiten – kommen *Neben-* oder *Seiteneffekte* hinzu. Solche Nebeneffekte sind einerseits nicht intendiert, andererseits aber nur schwer kontrollierbar. So ist etwa eine anlasslose Überwachung einer Gesellschaft mit der Regulierung von Kryptographie vielleicht nicht gewollt, denn intendiert ist *nur* die Aufdeckung von schweren Straftaten. Trotzdem kann ein weiterer Effekt einer solchen Regulierung sein, dass diese Überwachung trotz fehlender Intention *auch* die anlasslose Überwachung der Gesellschaft zur Folge hat. Das Missbrauchspotential ist somit ein Nebeneffekt, der in einer konsequentialistischen Argumentation bedacht werden muss. Besonders bedeutend wird dies dann, wenn in ursprünglich demokratisch-freiheitlichen Regionen eine solche Regulierung aufgrund der scheinbar rein positiven Folgen befürwortet wird.

Zusammenfassend zeigt das Verhältnis von Kryptographie und Konsequentialismus, dass sehr unterschiedliche ethische Argumente denkbar sind. Bislang war es hier nicht notwendig, sich für die eine oder andere Argumentation zu entscheiden. In den nachfolgenden Kapiteln, insbesondere Kapitel 6, werden solche Argumente allerdings spezifischer untersucht, um überzeugende konsequentialistische Antworten auf die Frage nach dem Umgang mit Kryptographie eruieren zu können. Aus dem vorliegenden Abschnitt ergeben sich für die folgenden Diskussionen einige Beispielfragen mit Blick auf einen konsequentialistischen respektive utilitaristischen Zugang zur Ethik der Kryptographie:

- Welchen Nutzen hat das Individuum durch die Anwendung der Kryptographie?
- Welche Vorteile lassen sich auf gesellschaftlicher Ebene erkennen?
- Welche Risiken entstehen durch den Einsatz von Identifikationstechnologien mithilfe kryptographischer Verfahren?
- Welche Probleme birgt eine allgemein verfügbare Kryptographie für Strafverfolgungsbehörden und die Justiz?

37 Siehe zur Diskussion des Panoptismus und des Panopticons etwa Ivan Manokha. „Surveillance, Panopticism, and Self-Discipline in the Digital Age". In: *Surveillance and Society* 16.2 (2018), S. 219–237; sowie Lyon, *The Electronic Eye*, S. 57–79.

– Welche Gefahr entsteht durch eine zentral kontrollierte und regulierte Kryptographie für Demokratien?
– Welches Missbrauchspotential besteht durch den Versuch, den Einsatz von Kryptographie für die vertrauliche Kommunikation zu beschränken?

Pflichtethik

Im Gegensatz zum Konsequentialismus klammert die Pflichtethik (oder Deontologie) bewusst die Folgen des menschlichen Handelns aus.[38] Für die Normativität einer ethischen Handlung oder Entscheidung spielt es keine Rolle, ob eine positive oder negative Konsequenz zu erwarten ist oder eintreten wird. Die moralische Richtigkeit einer Handlung ist dann gegeben, wenn jemand nach seinen *Pflichten* handelt oder entscheidet.[39] Die Pflichtethik kann damit auch als eine Antwort auf die Probleme des Konsequentialismus verstanden werden. Der einflussreichste Vertreter einer solchen Ethik war Immanuel Kant (1724–1804).

Kants gesamte Ethik hier wiederzugeben, wäre kaum zielführend. Insbesondere für die Begründung seiner Ethik ist auf die umfassende Literatur zu verweisen.[40] Dennoch lohnt es sich hier, einige Eckpunkte seiner Theorie auch auf den Umgang mit Kryptographie anzuwenden. Der Ausgang und die Bedingung für Kants Ethik ist der *gute Wille*.[41] Aufbauend darauf entwickelt Kant den *kategorischen Imperativ*.[42] Dieser ist zu unterscheiden von *hypothetischen Imperativen*: Ein hypothetischer Imperativ ist subjektiv und hängt von Zielen sowie von empirischen Bedingungen ab; demgegenüber ist ein kategorischer Imperativ allgemeingültig und unabhängig von einem Ziel.[43] Das höchste Prinzip der Moral ist nun

38 Siehe zur Einführung und zum Folgenden Wolff, *An Introduction to Moral Philosophy*, S. 163–199, zum Verhältnis von Kant zu Mill und dem Utilitarismus vor allem S. 163–164 sowie S. 167; siehe auch Deigh, *An Introduction to Ethics*, S. 140–146.

39 Siehe Fenner, *Ethik*, S. 172, sowie Pauer-Studer, *Einführung in die Ethik*, S. 36.

40 Siehe einführend zur Begründung des Kategorischen Imperativs etwa ebd., S. 44–49; weiterführend auch Ricken, *Allgemeine Ethik*, S. 133–149. Siehe zu Kants Ethik selbst Immanuel Kant. *Grundlegung zur Metaphysik der Sitten*. Hrsg. von Bernd Kraft und Dieter Schönecker. Hamburg: Felix Meiner Verlag, 1999.

41 Siehe Pauer-Studer, *Einführung in die Ethik*, S. 36–37.

42 Siehe einführend etwa Wolff, *An Introduction to Moral Philosophy*, S. 169–173.

43 Siehe einführend Ricken, *Allgemeine Ethik*, S. 134–136; Fenner, *Ethik*, S. 137–138; sowie Wolff, *An Introduction to Moral Philosophy*, S. 170–171.

Kant zufolge *der* Kategorische Imperativ im Singular: „*[H]andle nur nach derjenigen Maxime, durch die du zeitgleich wollen kannst, daß sie ein allgemeines Gesetz werde.*“[44] Kant nennt weitere Formulierungen des Kategorischen Imperativs, wobei eine davon – die Naturgesetzformel – lautet: „*[H]andle so, als ob die Maxime deiner Handlung durch deinen Willen zum allgemeinen Naturgesetze werden sollte.*“[45] Mit dieser Naturgesetzformel ist es möglich, zu testen, ob eine Maxime dem Kategorischen Imperativ genügt.[46]

Was würde ein deontologischer Ansatz für die Ethik der Kryptographie bedeuten – verglichen mit den bisher betrachteten konsequentialistischen Ansätzen? Illustrieren wir dies an einem Beispiel.[47] Dabei ist zu untersuchen, ob folgende Maxime der kantischen Ethik entsprechen würde: *Wenn es der nationalen Sicherheit dienlich ist, dann darf ein Staat oder ein Unternehmen eine garantiert private und vertrauliche Kommunikation abhören.* Auch wenn wir diese Maxime aus utilitaristischer Perspektive vielleicht annehmen würden, betrachten wir sie nun im Kontext der Naturgesetzformel. Können wir als Naturgesetz akzeptieren, dass eine garantiert private und vertrauliche Kommunikation abgehört werden darf, wenn es der nationalen Sicherheit dient? Die Antwort darauf *muss* negativ ausfallen. Eine Welt, in der garantiert private und vertrauliche Kommunikation abgehört werden darf, ist ein Widerspruch und nicht denkmöglich, insofern das Kriterium der garantierten Privatheit und Vertraulichkeit die Aktion des Abhörens ausschließt. Damit aber würde es sich um eine *vollkommene Pflicht* handeln, nicht nach dieser Maxime zu handeln.[48]

Es gibt aber auch im Kontext der Kryptographie weitere Fälle, bei denen eine deontologische Argumentation *schwächer* ist. Dies ist der Fall

44 Kant, *Grundlegung zur Metaphysik der Sitten*, S. 45, kursiv im Original. Siehe auch Fenner, *Ethik*, S. 138.

45 Kant, *Grundlegung zur Metaphysik der Sitten*, S. 45, kursiv im Original.

46 Siehe Ricken, *Allgemeine Ethik*, S. 141.

47 Die folgenden Schritte orientieren sich an Pauer-Studer, *Einführung in die Ethik*, S. 40–41, sowie Fenner, *Ethik*, S. 140–142. Die Analogie ist Kants Beispiel des lügenhaften Versprechens; siehe Kant, *Grundlegung zur Metaphysik der Sitten*, S. 46–47.

48 Siehe zu vollkommenen Pflichten Wolff, *An Introduction to Moral Philosophy*, S. 174; Pauer-Studer, *Einführung in die Ethik*, S. 40; sowie Fenner, *Ethik*, S. 139. Das analoge Beispiel Kants mit Blick auf falsche Versprechen ist ebenfalls diskutiert in Wolff, *An Introduction to Moral Philosophy*, S. 165–166.

bei sogenannten *unvollkommenen Pflichten*.[49] Betrachten wir dazu ein weiteres Urteil, bei dem wir uns folgende Situation vorstellen: Wir haben einen neuartigen Algorithmus entdeckt, der effizienter und sicherer ist als bisherige Verfahren. Die meisten Menschen könnten mit diesem Algorithmus sicherer und vertraulicher kommunizieren, als es ohne ihn der Fall ist. Die zu untersuchende Maxime lautet nun: *Wir dürfen den Algorithmus explizit geheim halten und nur für uns nutzen.* Ein solches Urteil mag intuitiv unproblematisch erscheinen, insofern es sich dabei schließlich um unseren eigenen Algorithmus handeln würde, über den wir doch wohl selbst entscheiden dürften.

Wenden wir nun aber erneut die Naturgesetzformel an.[50] Dadurch ergibt sich die Frage, ob die Maxime der Handlung zum Naturgesetz werden könnte – dass also niemand die eigens entwickelten Algorithmen über sein Umfeld hinaus teilen und veröffentlichen muss. Zunächst ist dieses Naturgesetz denkmöglich, da es keinen offensichtlichen Widerspruch gibt. Dies unterscheidet diese Maxime von der obigen Maxime über das Abhören von privater Kommunikation. Zur Argumentation ist aber folgende Präzision notwendig: Für Kant ist nicht nur das nicht Denkmögliche zu unterlassen, sondern auch das, was unserem eigenen Wollen widersprechen würde.[51]

Bei der oben betrachteten Maxime könnten wir argumentieren, dass es sich tatsächlich um einen solchen Widerspruch zum Wollen handelt, würden wir doch wollen, dass auch mit uns Algorithmen geteilt werden, die sicherer und effizienter sind als unsere eigenen. Das würde insbesondere in den Situationen gelten, in denen unser Algorithmus fehleranfällig ist und wir gleichzeitig keine Fähigkeiten haben, bessere Algorithmen zu entwickeln. Als Beispiel kann hier die Post-Quanten-Kryptographie dienen, die komplexere Mathematik und Implementierungen notwendig macht als beim DH-Schlüsselaustausch oder RSA.[52] Wir würden auch dort wollen, dass uns jemand in dieser Situation mit Algorithmen und vielleicht sogar deren Implementierung unterstützt. Für die obige Ma-

49 Siehe zu unvollkommenen Pflichten ebd., S. 174; Pauer-Studer, *Einführung in die Ethik*, S. 40–41; sowie Fenner, *Ethik*, S. 139–140.

50 Der folgende Absatz orientiert sich an der Analogie zu der Maxime, nach der wir uns nur um unser eigenes Wohlergehen kümmern müssten und nicht um das der Anderen. Dazu und zum Folgenden siehe Pauer-Studer, *Einführung in die Ethik*, S. 40–41.

51 Siehe ebd., S. 41.

52 Siehe zum Quantum Computing aus ethischer Perspektive auch Abschnitt 8.3.

xime, den Algorithmus explizit geheim zu halten, bedeutet das, dass das Handeln nach dieser Maxime zu unterlassen wäre.[53]

Die Umkehrung der Maxime wird aber begründbar: *Wir sollen unseren Algorithmus veröffentlichen und der Welt zugänglich machen.* Schließlich können wir erkennen, dass jeder Mensch einmal in der Situation sein dürfte, verschlüsselt kommunizieren zu wollen. Und aufgrund der enormen Komplexität der Modernen Kryptographie kann jener Mensch in dieser Situation nicht *alleine* die Algorithmen entwickeln, die dazu notwendig wären. Auch wir könnten (etwa in der Zukunft) nun ein solcher Mensch sein, wenn unsere eigenen Algorithmen veraltet und unbrauchbar werden würden; wir hätten in dieser Situation womöglich keine ausreichenden fachlichen Fähigkeiten, einen neuen, eigenen Algorithmus zu entwickeln.[54] Mit dieser Argumentation schafft dieses Beispiel sogar eine ethische Begründung für einen quelloffenen Ansatz von Software und Kryptographie (engl. *Open Source*).[55]

Diese zwei Maximen dürften für manche als Beispiele eines deontologischen Zugangs konstruiert wirken, womit die Kritikerinnen und Kritiker durchaus recht haben. Gerade ein deontologischer Ansatz weist die Schwäche auf, dass die konkreten Anwendungsfragen in den Hintergrund rücken und die Anwendbarkeit nicht immer eindeutig ist.[56] Ein solcher Zugang bedeutet aber auch, dass die Konsequenzen des Umgangs mit Kryptographie definitiv keine Rolle spielen. Ob nun das Wohl der Bevölkerung durch den Einsatz von zugänglicher Kryptographie steigt oder ob die öffentliche Sicherheit durch allgegenwärtige Verschlüsselung sinkt – all das wäre irrelevant. Im Alltag mag das wenig intuitiv scheinen. Bereits in Teil II wurde eruiert, dass die Folgen des Einsatzes (oder der Regulierung) von Kryptographie für das Individuum und die Gesellschaft

53 Es handelt sich hier damit nicht mehr um eine vollkommene Pflicht, sondern um eine unvollkommene Pflicht. Siehe zur Unterscheidung Wolff, *An Introduction to Moral Philosophy*, S. 174, sowie Pauer-Studer, *Einführung in die Ethik*, S. 40–41.

54 Eine solche Argumentation ist auch im Kontext der Menschenrechte mit dem *Prinzip der Verletzbarkeit* denkbar. Siehe Peter G. Kirchschläger. *Wie können Menschenrechte begründet werden? Ein für religiöse und säkulare Menschenrechtskonzeptionen anschlussfähiger Ansatz*. Münster: Lit Verlag, 2013, S. 273–335; sowie Peter G. Kirchschläger. „Das Prinzip der Verletzbarkeit als Begründungsweg der Menschenrechte". In: *Freiburger Zeitschrift für Philosophie und Theologie* 62 (2015).

55 Siehe allgemeiner und umfassender zu Open Source und dessen Kultur Coleman, *Coding Freedom*.

56 Siehe zum Anwendungsproblem Fenner, *Ethik*, S. 144, zur allgemeinen Kritik auch S. 144–146.

immens sind. Jedoch spielt es keine Rolle, ob dieser Ansatz im Alltagsverständnis intuitiv wäre. Für seine Attraktivität muss das nicht negativ sein, ganz im Gegenteil. Gerade *weil* eine solche Pflichtethik den Anspruch erhebt, die Konsequenzen auszuklammern, gewinnt sie Allgemeingültigkeit und Universalität.

Auch im Kontext der Pflichtethik lassen sich also unterschiedliche Argumente für eine Ethik der Kryptographie konstruieren. Insbesondere in Kapitel 7 werden wir uns im Kontext einer *egalitären Kryptographie* mit solchen Ansätzen auseinandersetzen. Beispiele für einen pflichtethischen bzw. deontologischen Zugang zu einer Ethik der Kryptographie wären folgende Fragen:

- Welche Pflicht haben Individuen, anderen die Möglichkeit zur vertraulichen und verschlüsselten Kommunikation zu ermöglichen?
- Sind auch Staaten in der Pflicht, die Rahmenbedingungen für ubiquitäre Verschlüsselungstechnologien bereitzustellen?
- Wie kann eine Pflicht zu implementierter Kryptographie begründet werden?
- Welche Pflichten haben Unternehmen beim Einsatz von Kryptographie, wenn dadurch eine allgegenwärtige Authentifizierung und Identifikation möglich werden?

Zusammenfassend wird deutlich, dass sowohl konsequentialistische als auch deontologische Zugänge zur Kryptographie möglich sind. Beide haben unterschiedliche Vor- und Nachteile in ihrer Anwendung auf die Kryptographie. Im politischen wie auch im wissenschaftlichen Diskurs scheint Kritik an einer ubiquitären Kryptographie häufig konsequentialistisch konnotiert zu sein (etwa aufgrund der nationalen Sicherheit). Befürworterinnen und Befürworter hingegen sehen sich aufgrund deontologischer Argumente bestärkt, für eine frei zugängliche und implementierte Kryptographie zu werben (etwa aus Perspektive der Privatsphäre). In Kapitel 6, Kapitel 7 und Kapitel 8 soll jedoch begründet werden, dass *beide* ethischen Zugänge für den Einsatz und die Nutzung der Kryptographie sprechen. Wir müssen uns für eine umfassende Ethik der Kryptographie daher nicht auf einen bestimmten ethischen Ansatz beschränken.[57] Eine

57 Für Kant würde es zwar keine Rolle spielen, ob das Handeln *auch* utilitaristisch geboten wäre; dies trägt, wie wir bereits diskutiert haben, nichts zur deontologischen Bewertung bei. Im Fall der angewandten Ethik können wir diese Offenheit jedoch methodisch beibehalten.

metaethische Abwägung, welcher der Zugänge nun der richtige sei, kann ausgeklammert werden, wenn beide für eine freie und zugängliche Kryptographie sprechen. Aber auch ein dritter Zugang, der spezifisch diskutiert werden soll, ist mit Blick auf die Menschenrechte möglich.

5.2 Menschenrechte und Kryptographie

David Kahn weist, wie bereits in Teil I diskutiert worden ist, in *The Codebreakers* auf eine Art kulturelle Universalität der Kryptographie hin: „It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously – as its parents, language and writing, probably also did.“[58] Der Drang nach kryptographisch sicherer Kommunikation in der ein oder anderen Form ist vielleicht gar ein Proprium anthropologischer Entwicklung. Kryptographie wäre damit aber nicht nur eine zufällige Sache, sondern würde genuin zur menschlichen Entwicklung gehören. Wenn wir uns diesen globalen und umfassenden Anspruch einer Modernen Kryptographie vor Augen führen, ist es nur naheliegend, auch die Menschenrechte als ethischen Zugang zur Kryptographie zu entwickeln.

So haben auch die Menschenrechte einen globalen Universalitätsanspruch.[59] Besondere Bedeutung erhalten die Menschenrechte dabei durch ihren *vorstaatlichen Charakter*: Sie werden nicht durch eine staatliche Gewalt gewährt oder erlaubt.[60] Der Staat hat vielmehr die Pflicht, entsprechend den Menschenrechten zu handeln und diese umzusetzen. Hinzu kommen bei Menschenrechten Merkmale wie etwa *angeboren und unverlierbar*, *egalitär* sowie *moralisch*.[61] Auf alle ihre Aspekte und Merkmale kann an dieser Stelle nicht eingegangen werden. Auch die Kritik an der

58 Kahn, *The Codebreakers*, S. 84; auch zitiert in Dooley, *History of Cryptography and Cryptanalysis*, S. 5.

59 Siehe Michael Lysander Fremuth. *Menschenrechte: Grundlagen und Dokumente*. Wien und Berlin: Verlag Österreich und Berliner Wissenschafts-Verlag, 2020, S. 26–31; sowie K. Peter Fritzsche. *Menschenrechte: Eine Einführung mit Dokumenten*. 3. Aufl. Paderborn: Ferdinand Schöningh, 2016, S. 22. Im Verhältnis zum Relativismus siehe Kerri Woods. *Human Rights*. Basingstoke und New York: Palgrave Macmillan, 2014, S. 104–123.

60 Siehe dazu und zum Folgenden Fremuth, *Menschenrechte*, S. 13–14, sowie Fritzsche, *Menschenrechte*, S. 19–20.

61 Siehe dazu die Auflistung bei ebd., S. 18–23.

Konzeption oder Existenz der Menschenrechte, die in der Literatur zahlreich vorgebracht worden ist, wird nicht näher diskutiert.[62]

Ähnlich wie zuvor soll auch hier ein pragmatischer Ansatz verfolgt werden, durch den mit den Menschenrechten ein weiterer ethischer Zugang zur Kryptographie möglich sein soll. Bei diesem Zugang werden die Menschenrechte als hypothetisch gegeben angenommen. Anschließend können wir eruieren, welche Menschenrechte für eine Ethik der Kryptographie von Bedeutung sind. Als dafür relevante Rechtsdokumente beziehen sich die folgenden Überlegungen auf die *Europäische Menschenrechtskonvention* (EMRK) sowie die *Allgemeine Erklärung der Menschenrechte* (AEMR).[63] Dieser Ansatz weist zwar die methodische Schwäche auf, dass die Menschenrechte an dieser Stelle nicht begründet werden. Dazu sei aber auf die ebenso umfassende Literatur verwiesen.[64]

Anders als bei den vorher diskutierten Zugängen zur Kryptographie aus ethischer Perspektive ist das Verhältnis von Kryptographie und Menschenrechten in der Forschung bereits umfassender beleuchtet worden.[65]

---

62 Siehe dazu einführend ebd., S. 24–25. Eine kritische Haltung nehmen MacIntyre und Rorty ein. Einführend zu diesen siehe Woods, *Human Rights*, S. 61–65; siehe im Original Alasdair MacIntyre. *After Virtue: A Study in Moral Theory*. 3. Aufl. Notre Dame: University of Notre Dame Press, 2007; sowie Richard Rorty. *Truth and Progress: Philosophical Papers*. Cambridge: Cambridge University Press, 1998.

63 Die AEMR ist abgedruckt in Fremuth, *Menschenrechte*, S. 202–206, die EMRK in ebd., S. 499–511. Weitergehend kann auch die Charta der Grundrechte der Europäischen Union (GRCh) für den europäischen Kontext hilfreich sein; siehe ebd., S. 590–599.

64 Siehe einführend zu den Menschenrechten Fritzsche, *Menschenrechte*, S. 24–25; Kirchschläger, *Wie können Menschenrechte begründet werden?*; sowie Michael Freeman. *Human Rights*. 2. Aufl. Cambridge und Malden: Polity Press, 2013. Siehe auch Andrew Clapham. *Human Rights: A Very Short Introduction*. 2. Aufl. Oxford: Oxford University Press, 2015; sowie Griffin, *On Human Rights*. Im Kontext der Ethik siehe zudem Konrad Hilpert. *Ethik der Menschenrechte: Zwischen Rhetorik und Verwirklichung*. Paderborn: Ferdinand Schöningh, 2019. Gleichsam bedeutet dieser Ansatz erneut, dass die Ethik der Kryptographie sich nicht ausschließlich auf einen Zugang beschränken muss.

65 Siehe insbesondere Wolgang Schulz und Joris van Hoboken. *Human rights and encryption*. Paris: UNESCO Publishing, 2016. URL: https://unesdoc.unesco.org/ark:/48223/pf0000246527 (besucht am 15.04.2024); sowie David Kaye. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/29/32. Human Rights Council, 2015. Siehe auch O. L. van Daalen. „The right to encryption: Privacy as preventing unlawful access". In: *Computer Law & Security Review* 49 (2023), Artikel 105804; Limniotis, „Cryptography as the Means to Protect Fundamental Human Rights"; Aisling Connolly. „Freedom of Encryption".

Einerseits dürfte dies am globalen und universellen Anspruch der Menschenrechte liegen, andererseits aber auch an einer inhaltlichen Verträglichkeit. Das naheliegendste, von der Kryptographie betroffene Recht ist hier nämlich das *Recht auf Achtung des Privat- und Familienlebens*.[66] In Artikel 12 der AEMR heißt es:

> Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre oder seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.[67]

Bei Artikel 12 fällt auf, dass es sich um eine *negative* Formulierung handelt, während die meisten Artikel der AEMR eine *positive* Formulierung aufweisen.[68] Für Böhm und Katheder bedeutet dies, dass mit dieser Art und Weise der Formulierung „einer der stärksten sprachlichen Ausdrücke verwendet worden [ist], um eindeutig festzusetzen, dass jemand ein Recht auf etwas hat, weil sie dieses Recht als gegeben voraussetzt“[69]. Gleichzeitig spezifiziert die AEMR hier die genannten Eingriffe als *willkürlich*. Die EMRK beinhaltet einen ähnlichen Artikel, wobei das Kriterium der Willkür nicht genannt wird. Auffällig ist aber, dass die EMRK einerseits

In: *IEEE Security & Privacy* 16.1 (2018), S. 102–103; sowie Daniel Kardefelt-Winther u. a. *Encryption, Privacy and Children's Right to Protection from Harm*. Innocenti Working Paper 2020-14. UNICEF, 2020. URL: https://www.unicef.org/innocenti/media/3446/file/UNICEF-Encryption-Privacy-Right-Protection-From-Harm-2020.pdf (besucht am 15.04.2024).

66 Häufig genannt ist in diesem Kontext der Kryptographie das Recht auf Privatsphäre sowie das Recht auf freie Meinungsäußerung. Siehe etwa Schulz und Hoboken, *Human rights and encryption*, S. 50–53. Spätere Arbeiten können daran anschließen und weitere Menschenrechte inkludieren, wie etwa die Würde des Menschen. Siehe dazu die Ausführungen bei van Daalen, der erkennt, dass „a broad range of rights in the human rights catalogue will also be affected by measures aimed at encryption technologies; think of the rights to human dignity, to respect for one's mental integrity, to freedom of thought, to assembly and to a fair trial. For all these rights, however, the link with encryption is more remote […]“; Daalen, „The right to encryption: Privacy as preventing unlawful access“, S. 8. Im Folgenden wird vor allem das Recht auf Privatsphäre sowie das Recht auf freie Meinungsäußerung spezifischer diskutiert.

67 Dokumentiert in Fremuth, *Menschenrechte*, S. 203.

68 Siehe Otto Böhm und Doris Katheder. *Grundkurs Menschenrechte: Die 30 Artikel. Kommentare und Anregungen für die politische Bildung*. Bd. 3. Würzburg: Echter Verlag, 2013, S. 40–42.

69 Ebd., S. 41.

wiederum *positiv* formuliert, andererseits aber dieses Recht in Artikel 8 Abs. 2 einschränkt:

> (1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
>
> (2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.[70]

Sowohl in der AEMR als auch in der EMRK betrifft dieses Recht den Schriftverkehr respektive die Korrespondenz, was insbesondere für den Fall der verschlüsselten Kommunikation relevant ist. Mit Blick auf eine Regulierung von verschlüsselter Kommunikation stellt sich zumindest bei Artikel 8 der EMRK aber die Frage, inwieweit Abs. 2 zum Tragen kommen könnte. Insbesondere die Einschränkung aufgrund der Verhütung von Straftaten sowie infolge von Erwägungen zur nationalen Sicherheit sind sprachlich wenig spezifisch und werden im Kontext einer Einschränkung von verschlüsselter Kommunikation immer wieder diskutiert.[71] Eine solche Abwägung im juristischen Sinne ist schließlich durch Gerichte zu treffen. Im Kontext des weiter unten besprochenen Rechts auf Meinungsfreiheit werden jedoch Möglichkeiten zu Eingriffen zu diskutieren sein. Deutlich wird in jedem Fall, dass die EMRK bei der Beschränkung des Rechts auf Privat- und Familienleben einen anderen Spielraum und konkretere Einschränkungsoptionen ermöglicht als die AEMR.

Einschränkungsoptionen wie diese sind im Kontext der Kryptographie letztlich auch sogenannte *latent ambiguities*, die Abschnitt 5.3 mit Blick auf Lessigs Ausführungen diskutieren wird. Die AEMR und die EMRK sind beide aus der Perspektive ihrer Zeit heraus verfasst worden. In dieser Zeit gab es eine ubiquitäre und globale Kryptographie, wie wir sie heute kennen, noch nicht. Bei einer brieflichen Korrespondenz ist ein spezifischer Eingriff in das Recht möglich, insofern eine Drittpartei den Brief bei der Poststelle öffnen könnte. Dies ist allerdings dann nicht mehr möglich, wenn die Kommunikation mit mathematischen Metho-

70 Zitiert nach Fremuth, *Menschenrechte*, S. 501.

71 Siehe Kapitel 6.

den und asymmetrischer Kryptographie erfolgreich verschlüsselt worden ist. Eine Ende-zu-Ende-Verschlüsselung verhindert, dass Nachrichten auf den Servern von Kommunikationsdienstleistern ausgelesen werden können. Unter diesen Umständen sind auch die entsprechenden Vorbehalte, Beschränkungen und Eingriffsmöglichkeiten neu zu diskutieren.[72] Für die Anwendung des Menschenrechts auf Achtung des Privatlebens ist daher festzuhalten: Der Kontext, der sich aufgrund technologischer Möglichkeiten wandelt, hat einen entscheidenden Einfluss darauf, wie Grund- und Menschenrechte umgesetzt werden können und sollten.

Um dies an einem weiteren Beispiel zu verdeutlichen: Was sagen die Menschenrechte im Hinblick auf sogenannte *Metadaten*? Wie sollten wir mit dieser Art von Daten umgehen dürfen? Sind solche Daten vor einem willkürlichen Eingriff zu schützen? Bei Metadaten handelt es sich um Daten, die zwar keine Inhaltsdaten sind, aber Informationen *über* die Kommunikation enthalten.[73] Dies wären etwa Daten dazu, *wann*, *mit wem* oder *wo* kommuniziert wird – nicht aber die Inhalte der Kommunikation. So gesehen ist womöglich ein Schutz dieser Metadaten zu verneinen, insofern sie nicht *direkt* durch das Menschenrecht auf Privatleben geschützt sind – schließlich sind Metadaten nicht Teil des verschlüsselten Inhalts. Auch in der brieflichen Kommunikation ist lediglich der Inhalt vertraulich, während die Anschrift (und ggf. auch der Absender) zur erfolgreichen Kommunikation von der Post lesbar sein müssen.

Allerdings können mit Metadaten und deren Aggregation Persönlichkeitsprofile erstellt werden.[74] Diese Profile können ähnlich viel über ein Individuum aussagen wie die Inhaltsdaten. Auch hier handelt es sich daher um eine *latent ambiguity*, die später spezifischer diskutiert wird und uns zu einer Entscheidung zwischen zwei sehr unterschiedlichen Konzeptionen zwingt. Der Europäische Gerichtshof für Menschenrechte in Straß-

72 Kapitel 6 wird zeigen, dass ein gezieltes Auslesen auf anderen Wegen möglich ist, etwa bei einem Zugriff auf die Endgeräte oder in Verbindung mit sogenannter *Spyware*. Dies allein bedeutet jedoch nicht, dass dadurch Spyware ethisch geboten wäre. Diese Diskussion wird in anderen Arbeiten zu führen sein.

73 Siehe einführend Jeffrey Pomerantz. *Metadata*. Cambridge, MA, und London: MIT Press, 2015; sowie Richard Gartner. *Metadata: Shaping Knowledge from Antiquity to the Semantic Web*. Cham: Springer, 2016, S. 1–2. Siehe auch Abschnitt 6.3.

74 Siehe zur Aggregation von Daten Daniel J. Solove. „A Taxonomy of Privacy". In: *University of Pennsylvania Law Review* 154.3 (2006), S. 477–564, S. 506–511. Eine solche Aggregation ist problemlos auch mit Metadaten möglich. Siehe dazu und zum Folgenden ausführlicher Abschnitt 6.3.

burg ist jedenfalls bereits seit 1984 der Ansicht, dass Metadaten einen Eingriff in Artikel 8 der EMRK darstellen können.[75] In Abschnitt 6.3 werden Metadaten und Menschenrechte im Kontext der Überwachung und Kryptographie genauer zu untersuchen sein.

Neben dem Recht auf Achtung des Privat- und Familienlebens ist im Kontext von Kryptographie insbesondere auch das *Recht auf Freiheit der Meinungsäußerung* betroffen, wie es in Artikel 19 der AEMR sowie Artikel 10 der EMRK niedergeschrieben ist. In Artikel 19 der AEMR heißt es:

> Jeder hat das Recht auf Meinungsfreiheit und freie Meinungsäußerung; dieses Recht schließt die Freiheit ein, Meinungen ungehindert anzuhängen sowie über Medien jeder Art und ohne Rücksicht auf Grenzen Informationen und Gedankengut zu suchen, zu empfangen und zu verbreiten.[76]

Artikel 10 Abs. 2 der EMRK benennt im Gegensatz zur AEMR, aus welchen Gründen das Recht auf Meinungsäußerung beschränkt werden kann. Auf den ersten Blick scheinen diese Gründe umfassend und oftmals treffend. Konkret heißt es dort:

> (2) Die Ausübung dieser Freiheiten ist mit Pflichten und Verantwortung verbunden; sie kann daher Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen unterworfen werden, die gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sind für die nationale Sicherheit, die territoriale Unversehrtheit oder die öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral, zum Schutz des guten Rufes oder der Rechte anderer, zur Verhinderung der Verbreitung vertraulicher Informationen oder zur Wahrung der Autorität und der Unparteilichkeit der Rechtsprechung.[77]

Diese Formvorschriften, Bedingungen, Einschränkungen oder Strafdrohungen müssen dabei *notwendig* (engl. *necessary*) sein. Die Messlatte für eine solche Notwendigkeit ist nach Ansicht des Europäischen Gerichtshofs für Menschenrechte nach dem Fall *The Sunday Times v. The United Kingdom* einigermaßen hoch:

---

75 Siehe Nora Ni Loideain. „EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era". In: *Media and Communication* 3.2 (2015), S. 55; sowie Paul Bernal. „Data gathering, surveillance and human rights: recasting the debate". In: *Journal of Cyber Policy* 1.2 (2016), S. 243–264, hier S. 248.

76 Dokumentiert in Fremuth, *Menschenrechte*, S. 204.

77 Dokumentiert in ebd., S. 502.

> The Court has noted that, whilst the adjective "necessary" […] is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" and that it implies the existence of a "pressing social need"[.][78]

Im Kontext der Kryptographie bedeutet dies: Die Existenz eines dringenden sozialen Nutzens stellt eine Hürde dar, die nicht automatisch erreicht wird, wenn *gewisse Vorteile* durch eine wie auch immer geartete Form der Beschränkung von Kryptographie erwartet werden können. Aus ethischer Perspektive handelt es sich eben nicht um eine *simple* Güterabwägung, bei der eine Bilanz nach Vor- und Nachteilen kalkulatorisch und arithmetisch zielführend sein könnte. Dadurch ist aber auch zu fragen, ob ein Eingriff in die Menschenrechte im Kontext der Kryptographie *überhaupt* irgendwann als notwendig gelten kann. Van Daalen erkennt dazu treffend:

> One of the requirements under human rights frameworks is that an interference is "necessary". If it is possible to gain access to unencrypted information without, for example, a policy aimed at weakening encryption technologies, an argument can be made that the policy is not necessary.[79]

Dies stellt also eine Hürde dar, die im Kontext der Kryptographie eine Art *Alternativlosigkeit* impliziert. Wenn es bereits *eine* mögliche und praktische Alternative gäbe, dann wäre das Kriterium der Notwendigkeit nicht mehr erfüllt. Wie van Daalen zudem richtigerweise erkennt, sind gerade solche Alternativen *trotz* verschlüsselter Kommunikation möglich, insofern ein System nur so sicher sein kann wie sein schwächstes Glied: Die Implementierung könnte einen Fehler enthalten, das Design des Algorithmus könnte fehlerbehaftet sein, die Schlüssel könnten einfach auszulesen sein.[80] Hinzu kommt, dass *direkte* Zugriffe auf die Endgeräte der Nutzenden die Möglichkeit einer Entschlüsselung und Ausnutzung von Schwachstellen erhöhen. Kapitel 6 wird schließlich zeigen, dass es sich bei jeder Verschlüsselung nur um eine *notwendige* Bedingung zur Sicherheit des Systems handelt – und eben nicht um eine *hinreichende* Bedingung. Im Kontext der Menschenrechte ist daher in begründeter Weise anzuzwei-

78 Siehe European Court of Human Rights. *The Sunday Times v. The United Kingdom*. Application no. 6538/74. 26. Apr. 1979, para. 59; besprochen und teilweise zitiert in Kaye, *A/HRC/29/32*, para. 34.

79 Daalen, „The right to encryption: Privacy as preventing unlawful access", S. 4.

80 Siehe ebd., S. 4.

feln, ob das Kriterium der Notwendigkeit bei den bisherigen Versuchen der Beschränkung und Regulierung von Kryptographie erfüllt ist.

Neben dieser Notwendigkeit steht das Recht auf Freiheit der Meinungsäußerung im engen Verhältnis zum Recht auf Achtung des Privatlebens. Oft wird dabei eine Balance gesucht, insofern in bestimmten Fällen beide Rechte im Konflikt zueinander stehen können.[81] So etwa im Journalismus, wenn diskutiert wird, ob die Freiheit der Meinungsäußerung eine öffentliche Aussage über das Privatleben von Personen des öffentlichen Lebens erlaubt.[82] Gleichwohl stehen beide Rechte nicht *ausschließlich* im Konflikt zueinander. Aus historischer Perspektive zeigt sich beispielsweise, dass das Recht auf Vertraulichkeit in Entwürfen der französischen *Déclaration des Droits de l'Homme et du Citoyen*[83] auftaucht – nicht aber wegen eines Rechts auf Privatsphäre, sondern vielmehr wegen des Rechts auf Freiheit der Meinungsäußerung.[84] In diesem historischen Kontext argumentiert Blanca R. Ruiz überzeugend, wie „the right to secrecy of telecommunications"[85] letztlich „the negative aspect of freedom of expression"[86] sei:

> For one thing, freedom of expression covers not only the freedom to choose when, how and about what we want to speak in public; it also covers the freedom to choose *whether* we want to speak in public at all. […] As a negative aspect of freedom of expression, secrecy of telecommunications guarantees that thoughts and opinions can be expressed in secret, which belongs to the realm of privacy.[87]

81 Siehe etwa Eric Barendt. „Balancing Freedom of Expression and Privacy: The Jurisprudence of the Strasbourg Court". In: *Journal of Media Law* 1.1 (2009), S. 49–72. Zur Beziehung beider Rechte zueinander auch Roger Toulson. „Freedom of Expression and Privacy". In: *The Law Teacher* 41.2 (2007), S. 139–154; John A. Humbach. „Privacy and the Right of Free Expression". In: *First Amendment Law Review* 11.1 (2012), S. 16–89; sowie Danutė Jočienė. „Freedom of expression and the right to privacy". In: *Teisė* 38 (2001), S. 7–19.

82 Siehe mit Blick auf das Verhältnis zum Journalismus ebd.; sowie Frederik J. Zuiderveen Borgesius und Wilfred Steenbruggen. „The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust". In: *Theoretical Inquiries in Law* 20.1 (2019), S. 291–322, hier S. 299.

83 Im Deutschen die *Erklärung der Menschen- und Bürgerrechte*.

84 Siehe Blanca R. Ruiz. *Privacy in Telecommunications: A European and an American Approach*. Den Haag: Kluwer Law International, 1997, S. 64–70, vor allem S. 67; zitiert und besprochen in Zuiderveen Borgesius und Steenbruggen, „The Right to Communications Confidentiality in Europe", S. 295.

85 Ruiz, *Privacy in Telecommunications*, S. 68.

86 Ebd., S. 68.

87 Ebd., S. 68, kursiv im Original.

Zudem ist die Verwirklichung des Rechts auf Meinungsäußerung oftmals abhängig vom Recht auf Achtung des Privatlebens. Man denke hier an den Fall, dass das Recht auf Achtung des Privatlebens eingeschränkt wird, indem etwa private Korrespondenz abgehört wird. In der Konsequenz ist zu erwarten, dass sich die korrespondierende Person anders verhält als in einer Situation, in der sie um den geschützten Rahmen der Kommunikation weiß. Sie wird geneigt sein, sich eher der Mehrheitsmeinung anzupassen. Sie wird sich insbesondere davor hüten, ihre Meinung zu äußern, wenn Konsequenzen zu befürchten sind. Ein solches Verhalten ist bekannt als der sogenannte *chilling effect* und kann als eine Art der Selbstzensur betrachtet werden.[88] Dazu genügt bereits die Möglichkeit oder Erwartung, abgehört und überwacht zu werden.[89] Denn die Person kann sich unter diesen Umständen in keinem Moment mehr sicher sein, ohne Aufzeichnung und ggf. Konsequenzen kommunizieren zu können.[90] *In der Konsequenz* widerspricht dieser Eingriff in die private Korrespondenz daher der Idee der Freiheit der Meinungsäußerung.

Auch aus einer rechtstheoretischen Perspektive zeigen Zuiderveen Borgesius und Steenbruggen präzise auf, wie das „right to communications confidentiality“[91] im Verhältnis zum Recht auf Meinungsäußerung

88 Siehe Moritz Büchi, Noemi Festic und Michael Latzer. „The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda“. In: *Big Data & Society* 9.1 (2022), S. 1–14; außerdem Jonathon W. Penney. „Internet surveillance, regulation, and chilling effects online: A comparative case study“. In: *Internet Policy Review* 2.6 (2017), S. 1–39; sowie Jonathon W. Penney. „Understanding Chilling Effects“. In: *Minnesota Law Review* 106 (2022), S. 1451–1530. Einführend zu allgemeiner Selbstzensur (im Englischen *Self-Censorship*) John Horton. „Self-Censorship“. In: *Res Publica* 17.1 (2011), S. 91–106; sowie Philip Cook und Conrad Heilmann. „Two Types of Self-Censorship: Public and Private“. In: *Political Studies* 61.1 (2013), S. 178–196. Zu einer qualitativen Studie auch Daragh Murray u. a. „The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe“. In: *Journal of Human Rights Practice* (2023), huad020.

89 Siehe Solove, „A Taxonomy of Privacy“, S. 494–495.

90 Die Parallele zum sogenannten *Panoptikum* von Jeremy Bentham ist offenkundig; siehe ebd., S. 495. Siehe auch Manokha, „Surveillance, Panopticism, and Self-Discipline in the Digital Age“; Penney, „Understanding Chilling Effects“, S. 1478–1487 und S. 1491; sowie Elizabeth Stoycheff u. a. „Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects“. In: *New Media & Society* 21.3 (2019), S. 602–619.

91 Zuiderveen Borgesius und Steenbruggen, „The Right to Communications Confidentiality in Europe“, S. 292.

und Privatsphäre steht.[92] Für sie stehen dabei beide Rechte nicht im Konflikt zueinander, sondern ergänzen sich gegenseitig:

> We argue that communications confidentiality is important, not only because it protects privacy but also because it protects other key values for the information society. By ensuring that individuals and businesses can freely exchange information and ideas with others, the right protects certain aspects of freedom of expression.[93]

Mit den Ausführungen von Ruiz sowie Zuiderveen Borgesius und Steenbruggen ergibt sich dann aber die Frage: Stellt eine Verletzung der Privatsphäre im Kontext von verschlüsselter Kommunikation womöglich sogar immer *auch* eine Verletzung des Rechts auf Meinungsäußerung dar?[94] Unabhängig von einer Beantwortung dieser Frage sind das Recht auf Achtung des Privatlebens und die Freiheit der Meinungsäußerung eng miteinander verbunden. Zusammenfassend sprechen aus einer menschenrechtsbasierten Perspektive das Recht auf Achtung des Privatlebens sowie das Recht auf freie Meinungsäußerung *für* den Einsatz von frei zugänglicher und ubiquitärer Kryptographie zur vertraulichen Kommunikation. Die jeweiligen Schranken und Einschränkungsoptionen sind in einer ethischen Analyse zwar zu bedenken, vermögen jedoch im konkreten Fall der Kryptographie nur wenig zu überzeugen. Wolfgang Schulz und Joris van Hoboken fassen in ihrer Studie *Human rights and encryption* daher auch zusammen:

> What ultimately matters, from a human rights perspective, is that cryptographic methods empower individuals in their enjoyment of privacy and freedom of expression, as they allow for the protection of human-facing properties of information, communication and computing. These properties include the confidentiality, privacy, authenticity, availability, integrity and anonymity of information and communication.[95]

Wie Schulz und van Hoboken richtigerweise feststellen, sind zudem all die anderen Schutzziele wie Integrität, Verfügbarkeit oder Authentizität im

92 Siehe ebd.

93 Ebd., S. 293.

94 Die umgekehrte Richtung ist dabei nicht betroffen. Eine Verletzung des Rechts auf Meinungsäußerung muss nicht zwangsläufig auch eine Verletzung der Privatsphäre darstellen.

95 Schulz und Hoboken, *Human rights and encryption*, S. 60.

Verhältnis von Kryptographie und Menschenrechte zu bedenken.[96] Diese gehen somit über das reine Schutzziel der Vertraulichkeit hinaus. Auch David Kaye, damaliger UN-Sonderberichterstatter für Meinungsfreiheit, verweist auf die Sicherheitskonzepte, die hinter Verschlüsselung und Anonymität stehen:

> Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity.[97]

Die kommenden Kapitel werden daher nicht nur aus einer Perspektive von Privatsphäre bzw. *Privacy* argumentieren, sondern auch umfassender im Sinne der Kryptographie als Hilfsmittel zur Realisierung des Rechts auf Freiheit der Meinungsäußerung und der digitalen Informationssicherheit. Sofern sich die Argumente im Folgenden nicht explizit auf das Recht auf Achtung des *Privatlebens* beziehen, wird aufgrund unterschiedlicher Übersetzungsmöglichkeiten meist der pragmatische englische Begriff *Privacy* verwendet, so wie er in der zahlreichen englischsprachigen Literatur üblich geworden ist.[98]

Auch wenn nun sowohl das Recht auf Achtung des Privatlebens als auch das Recht auf freie Meinungsäußerung für den Einsatz von Kryptographie sprechen, sind bislang andere Menschenrechte nicht in der Diskussion inkludiert worden. Ein Argument gegen den ubiquitären Einsatz von Kryptographie könnte nämlich etwa das Recht auf Leben und die Si-

96 Siehe Schulz und Hoboken, *Human rights and encryption*, S. 13.

97 Kaye, *A/HRC/29/32*, para. 56; teilweise auch zitiert in Schulz und Hoboken, *Human rights and encryption*, S. 28. Dabei handelte es sich um „UN's first authoritative in-depth account of the human rights status of encryption as well as anonymity"; ebd., S. 28.

98 Der Begriff wird im Sinne der überzeugenden Taxonomie von Daniel J. Solove verwendet; siehe Solove, „A Taxonomy of Privacy". Richtigerweise erkennt er nämlich an: „Privacy is too complicated a concept to be boiled down to a single essence. Attempts to find such an essence often end up being too broad and vague, with little usefulness in addressing concrete issues"; ebd., S. 485–486. Eine Diskussion, ob Privacy im Folgenden nun als *Privatsphäre*, *Privatleben*, *Privatheit* oder anderes übersetzt werden soll, kann mit dieser pragmatischen Nutzung des Begriffs *Privacy* umgangen werden. Anders ist dies, wenn es – wie beim Recht auf Achtung des Privatlebens – bereits *explizite* Übersetzungen gibt.

cherheit der Person sein. In Artikel 3 der AEMR heißt es schließlich, dass jeder Mensch „das Recht auf Leben, Freiheit und Sicherheit der Person“[99] hat. Mit diesem Recht könnte für die AEMR folgendes Gegenargument konstruiert werden:

> *Der Staat (oder ggf. ein Unternehmen) kann das Recht auf Leben und Sicherheit der Person nicht garantieren, wenn Kryptographie ubiquitär ist. Man denke hierbei nur an (X). Es muss also einen Trade-off geben zwischen Artikel 3 auf der einen Seite und Artikel 12 bzw. Artikel 19 auf der anderen Seite. Dieser Trade-off ist wegen der Natur der Kryptographie nur möglich, wenn es (Y) gibt.*

Für *(X)* ließen sich für gewöhnlich Beispiele aus dem Bereich des Terrorismus oder der Bekämpfung des organisierten Verbrechens einsetzen; für *(Y)* könnten wir denkbare Lösungen annehmen, wie die verpflichtende Implementierung von Backdoors oder das sogenannte Client-Side-Scanning. Ein solcher Trade-off, der die Realisierung der Menschenrechte für möglichst viele Menschen ermöglicht, wäre natürlich wünschenswert, wenn das Argument valide und konsistent wäre. Daran sind jedoch entscheidende Zweifel angebracht.[100] *Erstens* ist die Hypothese, dass das Recht auf Leben und Sicherheit der Person bei ubiquitärer Kryptographie nicht garantiert werden kann, realitätsfern. Wie bereits angedeutet, gibt es zahlreiche Methoden, die trotz des Einsatzes von Kryptographie einen Zugriff auf Endgeräte und die Daten ermöglichen.[101] *Zweitens* betreffen die Beispiele für *(X)* zumeist nicht das Gros der Bevölkerung. Die Gefahr und die Folgen terroristischer Anschläge oder des organisierten Verbrechens dürfen nicht verharmlost, sollten aber im Kontext der Alternative der anlasslosen Überwachung eingeordnet werden.[102] *Drittens* ist die Implikation des Arguments weitestgehend irreführend, insofern Sicherheit und Privacy nicht nur im Konflikt zueinander stehen. Kryptographie im

99 Dokumentiert in Fremuth, *Menschenrechte*, S. 203.

100 In Kapitel 6 werden diese Argumente insbesondere aus konsequentialistischer Perspektive eingehend zu diskutieren sein.

101 Siehe etwa die bereits genannten Aspekte bei Daalen, „The right to encryption: Privacy as preventing unlawful access“, S. 4.

102 Dies betrifft unter anderem die Überbetonung der negativen Folgen aufgrund kontextueller Spezifität. Siehe Shaun B. Spencer. „Security versus Privacy: Reframing the Debate“. In: *Denver University Law Review* 79.4 (2002), S. 519–521, 554, 571–573; diskutiert in Abschnitt 6.2.

Sinne der Informationssicherheit sorgt gerade *für* die (digitale) Sicherheit der Person.[103]

Es stellt sich dann aber zuletzt die Frage: Wenn das Recht auf Privatsphäre und das Recht auf Freiheit der Meinungsäußerung für den Einsatz von Kryptographie zur vertraulichen Kommunikation sprechen und gleichzeitig das Recht auf Leben und Sicherheit der Person kein überzeugendes Gegenargument darstellt, würde dann nicht auch ein *Menschenrecht auf Kryptographie* (engl: *right to encryption*[104]) naheliegen? Aus mehreren Gründen ist zumindest im Kontext dieser Arbeit Zurückhaltung geboten. Zunächst würden wir damit den zuvor beschriebenen methodischen Ansatz verlassen, bei dem wir von der hypothetischen Annahme der Menschenrechte nach AEMR und EMRK ausgegangen sind. In den vorherigen Überlegungen waren die Menschenrechte stets hypothetisch akzeptiert worden, wodurch ihr Verhältnis zur Kryptographie ohne eine Diskussion der Begründung der Menschenrechte bestimmt werden konnte. Ein *Menschenrecht auf Kryptographie* hingegen würde eine andere Methodologie erfordern, in der die Begründungsebene einzelner Menschenrechte zu inkludieren wäre. Ein solches Unterfangen ist methodisch nicht Teil der vorliegenden Arbeit, weshalb die bisherige Analyse nicht ohne Weiteres für eine voreilige Annahme eines Menschenrechts auf Kryptographie sprechen kann.

Hinzu kommt, dass die bisherige Argumentation deduktiver Natur war: Ausgehend von einem Recht auf Achtung des Privatlebens und einem Recht auf Freiheit der Meinungsäußerung kann erkannt werden, dass eine frei zugängliche und unbeschränkte Kryptographie als Voraussetzung der vertraulichen Kommunikation die Konsequenz dieser Menschenrechte ist. Durch diese Deduktion ist Kryptographie als Mittel zur verschlüsselten Kommunikation bereits in den bisherigen Menschenrechten nach EMRK und AEMR enthalten.[105] Ob ein solches *Mittel* überhaupt den Anspruch auf eine explizite Erwähnung als Menschenrecht erhalten kann, wäre zunächst zu diskutieren. Außer Frage steht, dass in der öffentlichen Wahrnehmung dadurch die Bedeutung der Kryptographie wachsen

103 Siehe für die Gründe auch Kapitel 6.

104 So etwa genannt bei Daalen, „The right to encryption: Privacy as preventing unlawful access".

105 So ist etwa für Limniotis Kryptographie „the Means to Protect Fundamental Human Rights"; Limniotis, „Cryptography as the Means to Protect Fundamental Human Rights".

dürfte. Aber ob ein solches konsequentialistisches Argument zur Begründung eines Menschenrechts auf Kryptographie ausreichen würde, wäre abermals Teil einer Auseinandersetzung auf Begründungsebene. Im Allgemeinen scheint für eine universelle Akzeptanz der Menschenrechte wohl ein konservativer und zurückhaltender Ansatz angesichts der Rufe nach *immer mehr expliziten Menschenrechten* sinnvoll.

Zum Abschluss dieser Einführung in das Verhältnis von Menschenrechten und Kryptographie ist auf eine Metaperspektive hinzuweisen, die auf die Ermöglichung der Realisierung der jeweiligen Menschenrechte im Kontext der Kryptographie blickt. Zu Beginn dieses Abschnitts ist von einer *Vorstaatlichkeit* der Menschenrechte gesprochen worden. Bislang ist aber das spezifische Verhältnis des Staates zu den Menschenrechten nicht eruiert worden. Fremuth fasst dieses zweischneidige Verhältnis im Kontext der Vorstaatlichkeit wie folgt zusammen:

> Einerseits gilt es, die Menschenrechte als vorstaatliche Rechte gegenüber dem Staat in Stellung zu bringen und dessen Gewalt zu „zähmen". Andererseits ist anzuerkennen, dass dem Staat zunehmend eine Leistungs- und Schutzgarantenpflicht zukommt, kraft derer er gehalten ist, den Genuss der Menschenrechte durch die Bereitstellung von Leistungen oder die Gewähr von Schutz zu ermöglichen.[106]

Diese „Janusköpfigkeit des Staates im modernen Menschenrechtssystem"[107] wird auch im Kontext der Kryptographie deutlich. Die Cypherpunks waren, wie Teil II diskutiert hat, dem Staat gegenüber zumeist kritisch eingestellt oder gar feindlich gesinnt. Der US-amerikanische Staat hingegen hatte es in den Crypto Wars oft als seine (vielleicht allzu große) Pflicht angesehen, Verschlüsslung regulieren zu müssen, um Unheil durch diese angebliche Anarchie der Kommunikation abzuwenden. Für diese gegenseitige Antipathie gibt es sicherlich nachvollziehbare Gründe, und die Moderne Kryptographie mit asymmetrischer Verschlüsselung und nachweisbarer Sicherheit stellt ein Novum in der Menschheitsgeschichte dar und erzwingt geradezu ein argumentatives Ringen um ihre Anwendung.

Nüchtern betrachtet greifen im Kontext der Menschenrechte solche dichotomen Ansichten über das Verhältnis von Kryptographie und Staat aber meist zu kurz. Es entspricht schließlich nicht der Realität, dass der

106 Fremuth, *Menschenrechte*, S. 14.
107 Ebd., S. 14.

Staat *immer* und *ausschließlich* Gegner der verschlüsselten Kommunikation sei. Gerade auch in demokratisch legitimierten Systemen *kann* der Staat zu dem Schluss kommen, dass Kryptographie aufgrund des Menschenrechts auf Achtung des Privatlebens und des Rechts auf freie Meinungsäußerung in der Kommunikation sogar zu fördern ist.[108] Das Briefgeheimnis kann als historisches Beispiel dienen, bei dem die private Kommunikation staatlich geschützt wurde.[109] Gleichzeitig ist der Staat aber auch in der Pflicht, diesen Schutz zu ermöglichen. Der Einschätzung von David Kaye, dem damaligen UN-Sonderberichterstatter für Meinungsfreiheit, kann daher abschließend nur zugestimmt werden:

> States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online.[110]

5.3 *Werte, Normen und latent ambiguities*

Im letzten Abschnitt der ethischen Zugänge zur Kryptographie beschäftigen wir uns mit *Werten* und *Normen*.[111] Werte und Normen können unterschiedlicher Natur sein. So gibt es etwa ökonomische Werte, soziale Normen und politische Werte, aber auch ethische Normen und Werte. Für unsere Diskussion ist im Sinne der Arbeit Letzteres von Interesse.

---

108 Siehe Daalen, „The right to encryption: Privacy as preventing unlawful access", S. 4–5.

109 Siehe einführend Ruiz, *Privacy in Telecommunications*, S. 64–67. Der Begriff *Briefgeheimnis* ist, wie Ruiz entsprechend herausarbeitet, sprachlich ungenau. Zumindest im Fall der Hessischen Verfassung waren nicht nur Briefe betroffen, sondern beispielsweise auch Pakete – gleichzeitig aber auch nur diejenige Korrespondenz, die über das Postsystem getätigt wurde. Siehe ebd., S. 65. Im Sinne sprachlicher Kohärenz im Deutschen wird im Folgenden jedoch weiterhin der Begriff *Briefgeheimnis* verwendet. Zur historischen Einführung siehe auch Zuiderveen Borgesius und Steenbruggen, „The Right to Communications Confidentiality in Europe", S. 293–297.

110 Kaye, *A/HRC/29/32*, para. 59.

111 Nach der Definition von Dagmar Fenner sind Werte „bewusste oder unbewusste Orientierungsstandards, von denen sich einzelne Individuen oder Gruppen in ihrem Verhalten leiten lassen". Moralische Normen hingegen sind „Handlungsregeln, die zu bestimmten Handlungsweisen im menschlichen Zusammenleben auffordern und den Anspruch auf allgemeine Verbindlichkeit erheben". Fenner, *Ethik*, S. 190.

Allerdings zielt dieser Abschnitt nicht darauf ab, einzelne relevante Werte oder Normen zu bestimmen. In den vorherigen Abschnitten sind bereits unterschiedliche ethische Zugänge zur Kryptographie eruiert worden, mit denen ethische Werte und Normen deduziert und diskutiert werden können. Was uns im Folgenden interessiert, ist eine *Meta*-Perspektive auf die Problematiken, die in der Anwendung in konkreten Situationen entstehen können. Um an das bereits oben herangezogene Beispiel anzuschließen: Was bedeutet das postalische Briefgeheimnis für die Vertraulichkeit der Kommunikation im Internet? Können wir die Norm des Briefgeheimnisses direkt auf die digitale Kommunikation übertragen? Oder treten hier bestimmte Anwendungsprobleme auf, die uns zu einer Diskussion der korrespondierenden Werte und des Briefgeheimnisses *selbst* zwingen? Um solche Fragen beantworten zu können, wird erneut Lawrence Lessigs *Code: Version 2.0* hilfreich sein.

Lessig weist in seiner Arbeit auf sogenannte *latent ambiguities* hin.[112] Solche unterschwelligen Zweideutigkeiten finden sich oft im Bereich der Technikethik, vor allem aber auch in der Frage nach dem Umgang mit Kryptographie. Für Lessig als Konstitutionalisten bedeuten diese *latent ambiguities*, dass in konkreten Fällen verschiedene Interpretationen konsistent mit der amerikanischen Verfassung sein können und wir uns für eine Interpretation (oder auch *translation*) entscheiden müssten.[113] Er formuliert dies wie folgt: „In the original context, the rule was clear […], but in the current context, the rule depends upon which value the Constitution was meant to protect."[114] Er zeigt dies am Beispiel eines Computerwurms, der andere Geräte ausspähen soll.[115] Wenn nun ein solcher Wurm eine positive Intention verfolgt, etwa jene, im Auftrag des FBI nach gestohlenen NSA-Dokumenten auf Speichergeräten zu suchen, dann stellt sich die Frage, ob dies der Konstitution widerstrebt oder nicht.[116]

Lessig nennt zwei denkbare Antworten: „It may be that we see the worm's invasion as inconsistent with the dignity the amendment was writ-

112 Siehe Lessig, *Code*, S. 25–26 sowie S. 157–168. Lessig zitiert hier in den Anmerkungen auch eine Definition von Samuel Williston; siehe ebd., S. 371–372, Anm. 28.

113 Siehe ebd., S. 25, zu *translation* siehe S. 157–168. Lessig bezeichnet sich selbst als Konstitutionalisten; siehe ebd., S. 4.

114 Ebd., S. 25.

115 Siehe ebd., S. 20–23. Im Gegensatz zum Virus fügt sich ein Wurm nicht an ein Programm an, sondern ist ein eigenständiges Stück Code; siehe Eckert, *IT-Sicherheit*, S. 65–66.

116 Siehe Lessig, *Code*, S. 20–23 sowie S. 25–26.

ten to protect“ [117] – oder aber wir erkennen „the invasion of the worm as so unobtrusive as to be reasonable“ [118]. Beide Varianten sind nach Lessig denkbar. Eine Durchsuchung per Wurm ist im Gegensatz zur physischen Durchsuchung unauffällig und unsichtbar. [119] Doch was bedeutet dies für die Bewertung des Wurms? Spricht es dafür, dass der Wurm als Durchsuchung im Sinne der Konstitution gelten sollte? [120]

Das Beispiel Lessigs zeigt, dass sich konkrete Antworten darauf, welches Handeln richtig und falsch, welches konsistent und welches inkonsistent ist, nicht immer *direkt* von bestimmten Normen, Konstitutionen oder Verträgen ableiten lassen. Besonders deutlich wird das, wenn Technologien neuartige Situationen ermöglichen, die zuvor gar nicht denkbar waren. Vor einigen hundert Jahren waren bestimmte Normen und Werte womöglich eindeutig und gaben in ihrer Anwendung wenig Anlass zu Diskussionen. Inzwischen hat sich der Kontext aber so radikal verändert, dass dadurch verschiedene Möglichkeiten denkbar werden. Lessig schreibt dazu:

> Changing contexts sometimes reveals an ambiguity latent in the original context. We must then choose between two different values, either of which could be said to be consistent with the original value. Since either way could be said to be right, we cannot say that the original context (whether now or two hundred years ago) decided the case. [121]

Auch wenn Lessig dies mehrheitlich mit Blick auf die Verfassung der USA und den amerikanischen Bezugsrahmen diskutiert, lässt sich diese Problematik im Sinne einer angewandten Ethik auch auf ethische Normen und Werte übertragen. Veranschaulichen wir dies an einem Beispiel, das an den vorangehenden Abschnitt zu den Menschenrechten anschließt und auch für die Kryptographie relevant ist. Der Menschenrechtsrat der Vereinten Nationen hat bereits mehrfach bekräftigt, „that the same rights that

117 Lessig, *Code*, S. 25.

118 Ebd., S. 25.

119 Siehe dazu und zum Folgenden ebd., S. 21.

120 Im Kontext des Abhörens weisen Whitfield Diffie und Susan Landau auf eine ähnliche Problematik hin, denn: „Unlike a search, the fact of whose occurrence is usually obvious, a wiretap is intrusive precisely because its invisibility to its victim undermines accountability.“ Diffie und Landau, *Privacy on the Line*, S. 4.

121 Lessig, *Code*, S. 165.

people have offline must also be protected online“ [122]. Was auf den ersten Blick selbstverständlich scheint, ist bei einer genaueren Analyse nicht mehr so eindeutig anwendbar. Oftmals können Gesetze, Normen und Rechte, wie sie in der Offline-Welt seit vielen Jahren akzeptiert werden, nicht ohne eine *fundamentale* Adaption auf die Online-Welt übertragen werden – *fundamental* deswegen, weil ein völlig neuer Kontext oft keine Alternative zulässt, als die Gesetze, Werte und Normen *selbst* zu diskutieren.

Das Briefgeheimnis kann hier erneut als Beispiel dienen: Ist aus ethischer Perspektive eine Anwendung auch auf die digitale Kommunikation möglich? [123] In einer Zeit, in der die kryptographische Anwendung lediglich dem Militär und der Diplomatie vorbehalten war, musste man sich mit solchen Fragen nicht auseinandersetzen. Der Paradigmenwechsel von der Klassischen Kryptographie hin zur Modernen Kryptographie erlaubte nun aber eine neue Art der individuellen Kommunikation, die zuvor niemand für möglich gehalten hatte. Wenn die Idee eines Rechts auf Achtung des Privatlebens in einer Zeit entwickelt wurde, in der Kryptographie noch nicht ubiquitär war, dann ist zu fragen, ob damalige Normen und Rechte auch auf die Moderne Kryptographie zu übertragen sind.

Um den Kontextwandel noch etwas genauer zu beschreiben: Vor 50 Jahren war die Vorstellung des Briefgeheimnisses und dessen Begründung eingebettet in eine andere Umwelt und eine andere technologische Realität. Da es naturgemäß keine sichere Barriere beim Briefverkehr gibt, die Schutz vor einem Abhören oder Lesen durch Dritte bietet, wurde eine Norm oder ein Gesetz nötig. Ein Zuwiderhandeln ist damit gesellschaftlich geächtet und zudem unter Strafe gestellt. Dieser Kontext hat sich im Bereich der Kryptographie geändert. In früheren Zeiten war ein Schlüsselaustausch zwischen den Kommunikationsparteien über einen weiteren, sicheren Kanal notwendig, um vertraulich mittels (Klassischer) Kryptographie kommunizieren zu können. Die Kryptographie beschränkte sich in ihrem Schutzziel der Vertraulichkeit auf die *symmetrische* Kryptographie. Erst mit der *asymmetrischen* Kryptographie ist es möglich geworden, über unsichere Kanäle Schlüssel auszutauschen, ohne einem stark hierarchischen System des Schlüsselmanagements vertrauen zu müssen.

122 Human Rights Council, *A/HRC/RES/20/8*, S. 2; siehe auch Human Rights Council, *A/HRC/RES/42/15*, S. 4.

123 Siehe zur kritischen Auseinandersetzung mit dem Begriff des Briefgeheimnisses Abschnitt 5.2; außerdem Ruiz, *Privacy in Telecommunications*, S. 65.

Der weitere Kontextwandel fand mit der Realität des Internets und der Rechenleistung statt, wodurch ein grundlegend anderer Kommunikationskanal entwickelt wurde, als der Briefverkehr ihn bot. Erst die gesteigerte Rechenleistung ermöglichte es, kryptographische Verfahren auf Endgeräten ubiquitär werden zu lassen. Während die Vertraulichkeitsgarantie beim unverschlüsselten Briefverkehr nicht über einen geschlossenen Briefumschlag oder ein geschlossenes Paket hinausgeht, ermöglichen Anwendungen im Internet durch die alltägliche Verwendung von Kryptographie eine vertrauliche Kommunikationsstruktur für alle – und das *by design*. Mit *by design* ist an dieser Stelle gemeint, was Lessig unter der Modalität der Architektur zusammenfasst: Kommunikation im Internet könnte prinzipiell auch ohne Kryptographie erfolgen.[124] Im Design der kryptographischen Anwendungen sind aber bestimmte Werte und Normen eingearbeitet. Oder wie es Lessig nennt: „code embeds values"[125].

Das Briefgeheimnis mag vielleicht rechtlich konstituiert sein, die Kryptographie hingegen entspringt der Mathematik. Nicht mehr der Schutz durch das Gesetz oder die gesellschaftliche Ächtung durch Normen sind für eine vertrauliche Kommunikation notwendig. Die bisher physische und unsichere Barriere eines Briefumschlags wird nun ersetzt durch die mathematische und sichere Kryptographie. Die kryptographisch gesicherte Online-Welt unterscheidet sich somit fundamental von der rechtlich normierten Offline-Welt. Verschlüsselte Kommunikation wird zum Status quo und zur architektonischen Garantie. Genau solche Fragen und *neuartigen* Problemstellungen führten letztlich zu den politischen Diskussionen über die Kryptographie in den 1990er-Jahren.[126]

Um damit auf Lessigs Kernaussage zurückzukommen: Eine *latent ambiguity* zwingt uns, zwischen zwei sehr unterschiedlichen Konzeptionen von Normen und Werten zu unterscheiden – im Kontext der Kryptographie exakt das, wozu uns auch der Paradigmenwechsel der Kryptographie zwingt.[127] Normen und Werte, die aus dem Paradigma der *Klassischen Kryptographie* stammen, sind nicht immer direkt auf das Pa-

124 Siehe auch Lessigs „difference by design"; Lessig, *Code*, S. 34.

125 Ebd., S. 114.

126 Siehe Diffie und Landau, *Privacy on the Line*, S. 12–13.

127 Siehe Lessig, *Code*, S. 155. Lessig nennt hierbei als Beispiel Privacy und den Vierten Zusatzartikel der amerikanischen Verfassung. Indem er die Ursprünge des Gesetzes beleuchtet, wird der Kontext ersichtlich, in dem ein solches Gesetz notwendig wurde. Siehe ebd., insbesondere S. 159–162.

radigma der *Modernen Kryptographie* anwendbar. Damit sieht sich aber auch der Staat vor neue Herausforderungen gestellt. Bei der brieflichen Kommunikation wäre ein Öffnen des Briefumschlags trotz bestehender Normen und Gesetze problemlos möglich. So kennt, wie bereits diskutiert worden ist, auch die EMRK Gründe dafür, das Recht auf Achtung der Korrespondenz beschränken zu dürfen. In der Praxis allerdings lässt sich eine Beschränkung der vertraulichen postalischen Kommunikation nicht in prozedural gleicher Weise auf die Kommunikation mithilfe kryptographischer Methoden anwenden. Eine Verschlüsselung, die nur *ein gewisses Maß* an Vertraulichkeit bietet, gleichzeitig einen Gesetzesvorbehalt implementiert und trotzdem *sicher* ist, ist aus kryptographischer Sicht nicht machbar.[128] Darüber hinaus lässt sich mit Lessig fragen: „How do we read a text written against a background of certain presuppositions when those presuppositions no longer apply?“[129]

Es ist nicht das Ziel dieses und der kommenden Kapitel, Lessigs stark konstitutionalistisch orientierte Argumentation zu übernehmen. Sein methodischer Grundgedanke lässt sich jedoch, wie das Beispiel des Briefgeheimnisses gezeigt hat, auch auf die Ethik und die Kryptographie anwenden. Denn gerade hier können wir fragen, welche Argumente und Werte für die Normen, Konventionen und Verfassungen *ursächlich* sind. Anschließend lässt sich mit Blick auf die generellen Möglichkeiten und Rahmenbedingungen von Technologie auch bewerten, welcher Umgang mit Technologie ethisch geboten ist. Dies alles bedeutet gerade nicht, dass etwa das Briefgeheimnis nicht als Referenz genutzt werden kann, um auch über verschlüsselte Kommunikation im Internet nachzudenken. Eine Eins-zu-eins-Übertragung jedoch wäre zu stark vereinfachend und würde den Kontext der neuen Technologie außer Acht lassen.

Die folgenden Argumentationen und ethischen Analysen gehen daher davon aus, dass die gleichen Rechte offline wie online geschützt werden *sollten*. Dies ist zu unterscheiden von einer Maxime, nach der die Rechte online auf gleiche Weise geschützt werden *müssen*, wie dies offline der Fall ist: Ein prinzipielles *Müssen* lässt keinen Raum zur Anpassung an die Realität – eine Online-Realität, die so fundamental verschieden ist von einer Offline-Realität, dass ein *Müssen* nicht möglich ist. Hingegen kann

128 Siehe vor allem die Diskussion in Abschnitt 6.3 und Abschnitt 7.1.

129 ebd., S. 160. Eine Frage dabei ist, ob der Vierte Zusatzartikel der amerikanischen Verfassung Verschlüsselung oder Privacy inkludiert, was auch Jarvis diskutiert; siehe Jarvis, *Crypto Wars*, S. 7.

ein normatives *Sollen* an der Machbarkeit und Realisierbarkeit, an den realen Umständen in der Anwendung scheitern. Wenn Letzteres der Fall ist, können wir anschließend auf ethisch-rationaler Basis eruieren, wie die Rechte, die die Menschen offline haben, auch *bestmöglich* online geschützt werden können.

Damit wird nun ersichtlich, warum sich die vorliegende Arbeit bislang so intensiv mit den Möglichkeiten der Kryptographie beschäftigt hat. Auch wenn klar sein dürfte, dass die Werte und Normen, die bislang nur offline angewendet wurden, auch online gelten sollten, bedeutet dies nicht, dass sie auch in der tatsächlichen Praxis umsetzbar sind. In diesem Zusammenhang ist auf die pragmatische Methodik der Argumentation und die Diskussion um ein *Bottom-up-* vs. ein *Top-down*-Modell einer anwendungsorientierten Ethik zurückzukommen.[130]

Das rigorose Top-down-Modell geht von bestimmten Werten und Normen aus, die womöglich auch in Deklarationen oder Konstitutionen festgehalten wurden. Schnell wird aber ersichtlich, dass die Anwendbarkeit dieses Top-down-Modells an der Realität scheitert. In Verbindung mit einem Bottom-up-Modell kann jedoch auch die konkrete Situation respektive Realität zur Erkenntnisfindung beitragen.[131] Damit orientiert sich diese Arbeit einerseits an der Realität, die als beschränkender Rahmen gelten muss. Andererseits herrscht *innerhalb* dieses Rahmens keine Beliebigkeit vor. Vielmehr ist in ihm zu fragen, wie mit neuen Technologien umgegangen werden sollte. Mit Lessigs *latent ambiguities* können wir auch im Kontext der Kryptographie eruieren, wie der Umgang mit neuer Technologie ethisch zu gelingen vermag.

Methodisch handelt es sich also um eine dialektische Argumentationsstruktur. Wenn die Deduktion von Normen an der Realität schei-

130 Siehe Abschnitt 5.1. Bei einem Top-down-Modell werden universelle Prinzipien auf den konkreten Anwendungsfall übertragen. Im Bottom-up-Modell hingegen werden Werte und Normen auch aus den Erfahrungen der konkreten Situation induziert. Siehe zur Einführung in die Ansätze Fenner, „Angewandte Ethik zwischen Theorie und Praxis", S. 100–101, bzw. Fenner, *Einführung in die Angewandte Ethik*, S. 10–12; ebenso Filipović, „Angewandte Ethik", S. 123–124.

131 Das Verhältnis zwischen der konkreten Ausgangslage auf der einen Seite und den Intentionen von Werten und Normen auf der anderen Seite ist aber nicht immer einfach zu bestimmen. Wenn etwa aufgrund der technologischen Realität zwei sehr unterschiedliche Möglichkeiten des Umgangs mit jener Technologie zur Disposition stehen, welche ist dann zu wählen? Kann eine Balance gelingen, die die Umsetzung beider Möglichkeiten anstrebt?

tert, dann zwingt dies zur Überprüfung der generellen Anwendbarkeit und Sinnhaftigkeit der Normen. Wenn etwa eine Art Gesetzesvorbehalt für die Kryptographie implementiert werden muss und gleichzeitig das Recht auf vertrauliche Kommunikation gewahrt werden soll, dann ist zu erkennen, dass dies aufgrund der Realität nicht umsetzbar ist. Darauf aufbauend ist ethisch zu diskutieren, ob der Gesetzesvorbehalt aufgegeben oder geändert werden sollte oder ob wir das Recht auf eine vertrauliche Kommunikation anlasslos und generell einschränken wollen. Solche Entscheidungen darüber, welchen ursprünglichen Werten wir folgen, sind in den nächsten Kapiteln zu diskutieren.

In all diesen Entscheidungen sollen Mittel und Wege gesucht werden, wie die *Intention* ursprünglicher Normen bestmöglich im Sinne der korrespondierenden Werte realisiert werden kann. Im Kontext der Kryptographie etwa wäre ein Auslesen der Nachrichten zwar nicht per Fernzugriff oder auf Servern möglich. Mit hoher Wahrscheinlichkeit könnten Behörden aber zielgerichtet und anlassbezogen Kommunikation auslesen, wenn sie einen physischen Zugriff auf die Endgeräte haben. Damit bliebe einerseits das Recht auf vertrauliche Kommunikation gewahrt, andererseits gäbe es in begründeten Fällen stets die Möglichkeit, per richterlichem Beschluss Analysen der Endgeräte durchzuführen.

Eine solche Argumentation verbindet die Realität neuartiger Kontexte mit den Zugängen zur Ethik der Kryptographie. Dazu werden in den folgenden Analysen pflichtethische und konsequentialistische Begründungen genannt, aber auch auf menschenrechtsbasierte Ansätze der vertraulichen Kommunikation kann verwiesen werden. Gerade eine solche Synthese spricht für die interdisziplinäre Bedeutung der Ethik der Kryptographie: *Latent ambiguities* erzwingen eine gut begründete und anwendungsorientierte Ethik, da andernfalls entweder Beliebigkeit oder Realitätsverweigerung droht.

6 Zielkonflikte und (Schein-)Dichotomien

> Und warum sind sie so fest, so feierlich davon überzeugt, daß einzig das Normale und Positive, mit einem Wort: nur die Glückseligkeit für den Menschen vorteilhaft sei?
>
> – Fjodor Dostojewskij in *Aufzeichnungen aus dem Kellerloch*[1]

Das vorherige Kapitel hat gezeigt, dass bei einer ethischen Analyse sogenannte *latent ambiguities* auftauchen können.[2] Sie zwingen uns, zwischen sehr unterschiedlichen Konzeptionen und Umsetzungen von Werten und Normen zu differenzieren. Wenn nun zwei (oder mehr) dem Anschein nach inkompatible Möglichkeiten und Ziele zum Handeln und zum Entscheiden zur Disposition stehen, dann bezeichnet die Ethik das als *Zielkonflikt*. Beispielsweise scheint uns die Moderne Kryptographie zu zwingen, im Rahmen von vertraulicher Kommunikation abzuwägen, ob und wann wir das Recht auf Achtung des Privatlebens höher gewichten als das Recht auf Leben. Das wäre, so das Argument, etwa der Fall, wenn es sich um Themen der nationalen Sicherheit oder Terrorismusbekämpfung handeln würde. Zielkonflikte sind aber nicht nur im Bereich der (Menschen-)Rechte zu verorten, sondern oft auch bei unterschwellig konsequentialistischen Ansätzen. So geht es bei in Konflikt zueinander stehenden Zielen um die Frage, welche Konsequenzen *besser* oder *wünschenswerter* seien als andere.

Solche ethischen Zielkonflikte sind die Folge von (Schein-)Dichoytomien – einer Zweiteilung von Handlungsoptionen. Diese Zweiteilungen unterstützen meist Argumente, die *gegen* eine freie, ubiquitäre und globale Kryptographie sprechen. Für die Überzeugungskraft einer Ethik der Kryptographie hilft es daher zu analysieren, wann solche Dichotomien wirklich existieren – und wann es sich lediglich um *Schein*-Dichotomien handelt. Schein-Dichotomien können beispielsweise auf falschen Prämissen, einem mangelnden Realitätsbezug oder einer ethischen Widersprüchlichkeit aufbauen. Die folgenden Kapitel werden zeigen, dass eine

1 Fjodor Dostojewskij. *Aufzeichnungen aus dem Kellerloch*. 9. Aufl. Aus dem Russsischen von Swetlana Geier. Frankfurt am Main: Fischer Taschenbuch, 2023, S. 40.

2 Siehe zu den *latent ambiguities* Lessig, *Code*, S. 25–26 sowie S. 157–168.

Identifikation der *tatsächlichen* Dichotomien und eine Offenlegung der nur *scheinbaren* Dichotomien bereits zahlreiche, oftmals konsequentialistische Gegenargumente hinsichtlich einer freien, ubiquitären und globale Kryptographie zur vertraulichen Kommunikation zu widerlegen vermögen. Abschnitt 6.1 wird dazu eruieren, dass Kryptographie *nicht* als Dual-Use-Technologie klassifiziert werden sollte; Abschnitt 6.2 wird argumentieren, dass es *keine* Dichotomie von Privacy vs. Sicherheit gibt; und Abschnitt 6.3 wird zuletzt analysieren, dass Überwachung *trotz* Kryptographie möglich ist.

6.1 Kryptographie und Dual Use

Eine sogenannte *Dual-Use-Technologie* ist eine Technologie, die sowohl für zivile als auch für militärische Zwecke genutzt werden kann.[3] Oftmals wird bei Exportbeschränkungen von einem solchen Dual-Use-Charakter gesprochen. Davon betroffen ist auch die Kryptographie, etwa mit dem *Wassenaar-Abkommen* (engl. *Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies*).[4] Auch vor dem Wassenaar-Abkommen war Kryptographie immer wieder im Rahmen von Exportbeschränkungen diskutiert worden, insbesondere in den USA durch den *Export Administration Act* (EAA).[5] Mit dieser Bedeutung des Dual-Use-Charakters handelt es sich um die erste Dichotomie, bei der wir die Frage stellen müssen: Ist Kryptographie wirklich eine Dual-Use-Technologie?

3 Zu einer aktuellen Einführung siehe Riebe, *Technology Assessment of Dual-Use ICTs*. Diese Arbeitsdefinition ist bewusst wenig spezifisch und soll ausschließlich auf die Grunddifferenz der Ziele hinweisen. Auch international existiert keine abschließende Definition des *Dual-Use*-Begriffs; siehe Veronica Vella. „Is There a Common Understanding of Dual-Use? The Case of Cryptography". In: *Strategic Trade Review* 3.4 (2017), S. 103–122.

4 Siehe einleitend Riebe, *Technology Assessment of Dual-Use ICTs*, S. 137, sowie Thea Riebe u. a. „U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance". In: *European Journal for Security Research* 7.1 (2022), S. 39–65, S. 43.

5 Siehe einführend Diffie und Landau, *Privacy on the Line*, S. 120–123. Einleitend zu Kryptographie und Dual-Use aus Policy Perspektive auch Vella, „Is There a Common Understanding of Dual-Use?"; im Kontext der Exportbeschränkungen auch Anderson, *Security Engineering*, S. 934–935.

Im Kontext der Kryptographie scheint *Dual Use* zunächst einen Zielkonflikt zu meinen, insofern auf der einen Seite eine positive Nutzung, auf der anderen Seite aber eine negative Nutzung steht, wenn wir hierbei zur Vereinfachung militärische Nutzung als negative oder auch gefährliche Nutzung klassifizieren wollen. Damit kann die Frage nach dem Dual-Use-Charakter zunächst verallgemeinert werden: Welchen *Nutzen* hat Kryptographie eigentlich? Einerseits liegen somit offenbar utilitaristische Argumente nahe. Andererseits sind aber auch anthropologische Perspektiven auf die Natur der Kommunikation und der Kryptographie denkbar. Wenn wir anschließend davon ausgehen würden, dass Kryptographie tatsächlich eine Dual-Use-Technologie wäre, sollte eine zweite Frage gestellt werden: *Wie* könnte Kryptographie als Dual-Use-Technologie beschränkt werden? Diese zweite Frage ist konzeptuell zu unterscheiden von der ersten Frage, da sie auf die Bedingungen der Möglichkeit einer Regulierung abzielt.

Kehren wir aber zunächst zur ersten Frage zurück: Welchen Nutzen hat Kryptographie? Handelt es sich bei ihr wirklich um eine Dual-Use-Technologie, weil sie sowohl militärisch als auch zivil genutzt werden kann? Auf den ersten Blick ist diese Frage offensichtlich mit *Ja* zu beantworten, insofern Kryptographie tatsächlich für beide Verwendungsarten von Nutzen ist. Wie Teil I deutlich gemacht hat, war Kryptographie ohnehin lange Zeit vor allem ein militärisches Werkzeug.[6] Kryptographie war bis dahin bei Weitem nicht so verbreitet, wie es heute der Fall ist. In einer Zeit, in der Kryptographie monopolisierbar war und von einigen wenigen monopolisiert wurde, entstand eine Asymmetrie zwischen denen, die Kryptographie nutzen konnten, und denen, die Kryptographie nicht nutzen konnten. Daher ist verständlich, dass in den 1980er- und 1990er-Jahren eine solche Vorstellung des Dual-Use-Charakters nahelag.

Aber um dieses Argument zunächst aus sozial-gesellschaftlicher und anthropologischer Perspektive zu kontextualisieren: Dual-Use-Güter existieren *überall*. Auch *Sprache* wird für das alltägliche Leben verwendet. Sprache ist eine menschliche und soziale Äußerungsform, die für ein gesellschaftliches Zusammenleben zumindest in der ein oder anderen Kommunikationsform üblich ist. Zugleich wird Sprache auch genutzt, um Kriege zu führen, Befehle zu erteilen, Propaganda zu verbreiten. Dennoch käme wohl kaum jemand auf die Idee, den Export von Kriegsvokabular und Übersetzungen zu beschränken.

6 Noch Kerckhoffs schreibt von der *militärischen* Kryptographie; siehe Kerckhoffs, „La Cryptographie Militaire".

Sicherlich handelt es sich hier um einen provokanten Vergleich. Sprache sei, so könnte eingewendet werden, schließlich eine natürliche Sache und keine digitale Technologie. Und doch ist die Analogie an vielen Stellen überraschend treffend, wenn wir Kryptographie und den menschlichen Drang nach vertraulicher Kommunikation eben auch als eine genuin *soziale Angelegenheit* betrachten. Nach David Kahns *The Codebreakers* musste ja gerade das menschliche Bedürfnis nach Privatsphäre in einer sozialen Umgebung zur Verschlüsselung führen.[7] Es ist zwar historisch richtig, dass Kryptographie nicht immer im gleichen Maße mathematisch und ubiquitär war wie heute. Ein gewisses Maß an Privatsphäre in der sozialen Umgebung scheint den Menschen aber doch anthropologisch zu begleiten. Vor dem 21. Jahrhundert ließ sich diese Privatsphäre herstellen, indem man sich (zeitweise) von der Gesellschaft zurückzog. Heute hingegen ist Kommunikation und die Ansammlung von Daten so allgegenwärtig, dass dieses Zurückziehen ohne kryptographische Unterstützung kaum mehr möglich ist. Auch Whitfield Diffie und Susan Landau analysieren diesen Kontext von Telekommunikation und privater Kommunikation:

> When telecommunication was merely an adjunct to physical communication, it was possible to hedge about privacy. When two people meet frequently as well as talking regularly by telephone, they can reserve indiscreet remarks for their face-to-face meetings. But as telecommunication becomes more the rule than the exception, this becomes less feasible. In a future society (which may not be far off) in which most communication is telecommunication and many close relationships are between people who never meet in person, it becomes impossible. If people are to enjoy the same effortless privacy in the future that they enjoyed in the past, the means to protect that privacy must be built into their communication systems.[8]

Kann vor diesem Hintergrund der Rückzug aus der Gesellschaft oder ein Gespräch von Angesicht zu Angesicht als Dual-Use-Akt klassifiziert werden? Verfechterinnen und Verfechter des Dual-Use-Charakters der Kryptographie würden hier argumentieren, dass vertrauliche kryptographische Kommunikation dem organisierten Verbrechen, militärischen Aktivitä-

7 Siehe Kahn, *The Codebreakers*, S. 84.

8 Diffie und Landau, *Privacy on the Line*, S. xvi–xvii. Oder um es in den Worten von Julian Assange zu sagen: „We now have increased communication versus increased surveillance. Increased communication means you have extra freedom relative to the people who are trying to control ideas and manufacture consent, and increased surveillance means just the opposite." Assange u. a., *Cypherpunks*, S. 21.

ten oder terroristischen Vereinigungen nützlich sei. Sicherlich ist dem zuzustimmen. Jedoch ändert dies nichts daran, dass auch die Möglichkeit des Rückzugs aus der Gesellschaft ein Dual-Use-Akt wäre. Was unterscheidet die verschlüsselte Kommunikation von einem Rückzug aus der Gesellschaft, sodass eine Klassifikation als Dual-Use-Technologie unausweichlich und *notwendig* ist?[9] Die Beweislast liegt hier aufseiten derer, die die Kryptographie mit einem Dual-Use-Charakter differenzieren wollen.

Diese provokante erste Antwort auf die Frage nach Kryptographie und Dual-Use-Technologien ist maßgeblich anthropologischer Natur und baut auf der Prämisse auf, dass jeder Mensch an dem ein oder anderen Punkt in seinem Leben den Drang nach vertraulicher Kommunikation verspürt. Dieses Verlangen lässt sich im 21. Jahrhundert nun aber nur durch kryptographische Verfahren befriedigen. Das legt den Schluss nahe, dass kryptographische Verfahren sozial-gesellschaftlich und anthropologisch erklärbar sind. Doch auch ohne diese Prämisse kann argumentiert werden, dass Kryptographie nicht als Dual-Use-Technologie klassifiziert werden *sollte*. Diese zweite Argumentation ist nicht mehr anthropologisch, sondern konsequentialistisch.

Kryptographie ist zunächst *essentiell* für die Sicherheit von digitaler Kommunikation und Technologie.[10] Unsichere Systeme hingegen sind eine Gefahr für die Sicherheit.[11] Die Beschränkung von Kryptographie hat somit einen negativen Effekt auf die digitale Sicherheit und damit auf das Individuum und die Gesellschaft.[12] Am deutlichsten wird dies an einem globalen Finanzsystem, bei dem unterschiedlichste Parteien an verschiedenen Orten auf der Welt in kurzer Zeit Geldbeträge transferieren müssen. Im Kontext von Exportbeschränkungen erhielt daher die Bankenindustrie, wenig überraschend, spezielle Exporterlaubnisse.[13] Daran, dass ubiquitäre Kryptographie zur Verschlüsselung auch die Sicherheit

9 *Notwendig* im Sinne der in Abschnitt 5.2 beschriebenen *Notwendigkeit* im Kontext der Menschenrechte.

10 Beispiele hierzu bei Beutelspacher, *Geheimsprachen und Kryptographie*, S. 113–114. Siehe auch im Kontext der Informationssicherheit Abschnitt 2.4.

11 Als ein weiteres Beispiel kann der Schutz von geistigem Eigentum dienen; siehe Landau, „The National-Security Needs for Ubiquitous Encryption", S. 2.

12 Siehe Aljifri und Sánchez Navarro, „International legal aspects of cryptography", S. 203.

13 Siehe Diffie und Landau, *Privacy on the Line*, S. 73 sowie S. 121.

von digitalen Systemen erhöht, kann aus technologischer Sicht nicht gezweifelt werden.[14]

Bei Kryptographie als Werkzeug technologischer Sicherheit handelt es sich um eine instrumentalistische Perspektive. Für eine Ethik der Kryptographie spielt aber auch die utilitaristische Frage eine Rolle, was Kryptographie in der indirekten und mittelbaren Konsequenz *gesellschaftlich* bewirken kann.[15] Beispiele aus der jüngeren Vergangenheit deuten darauf hin, dass Kryptographie oftmals zum Guten eingesetzt wird, so auch bei PGP:

> Activists from Myanmar used the encryption program [PGP] to hide communications from a brutal military junta that would kill its citizens for even owning a fax machine. A Bosnian user sent Zimmermann a message to say that during the siege of Sarajevo, his father had used PGP to encrypt e-mails to his family during the hour or two of occasional electricity in the war-torn city.[16]

Anekdotische oder exemplarische Evidenz ist keine überzeugende Evidenz. So können Gegenargumente vorgebracht werden, insbesondere das ebenso konsequentialistisch geprägte *Going-Dark-Problem*.[17] Bei diesem wird davon ausgegangen, dass Strafverfolgungsbehörden dank der Kryptographie *im Dunkeln herumtappen müssen*. Wenn zwei Kriminelle per verschlüsselter Kommunikation Pläne schmieden könnten, könne die Strafverfolgung sowohl präventiv als auch investigativ nur schwer bis gar nicht darauf reagieren. Mit dieser Argumentation würde das oben genannte Argument ausgehebelt: Ein Gespräch von Angesicht zu Angesicht

14 Ein Gegenargument hierfür könnten sogenannte *Ransomware*-Attacken sein, die bereits in Abschnitt 2.4 genannt wurden. Bei Ransomware versucht eine angreifende Partei, mittels Schwachstellen in ein System einzudringen, um die Daten anschließend zu verschlüsseln. Anschließend konfrontiert sie das Opfer mit einer Lösegeldforderung, oft verbunden mit der Androhung, die Informationen zu veröffentlichen, sollte der Forderung nicht nachgekommen werden. Hier kann allerdings die Kryptographie nicht als alleinige Ursache für den Erfolg von Ransomware identifiziert werden. Ganz im Gegenteil ist eine gezielte Verschlüsselung von Daten gerade das Werkzeug, mit dem solche Androhungen einer Veröffentlichung wirkungslos werden.

15 So ist Kryptographie etwa für den deutschen Mathematiker Albrecht Beutelspacher nicht nur generell *gut*, sondern das sind eben auch ihre Anwendung und ihre Algorithmen. Siehe Beutelspacher, *Geheimsprachen und Kryptographie*, S. 111.

16 Greenberg, *This Machine Kills Secrets*, S. 74.

17 Siehe einführend Gasser u. a., *Don't Panic*; vor allem auch Abschnitt 6.3.

könnte observiert und abgehört werden – dank des Going-Dark-Problems sei dies heute im digitalen, verschlüsselten Bereich nicht mehr möglich.

Dieses Gegenargument entspricht allerdings nicht der Realität, wie Abschnitt 6.3 ausführlicher darlegen wird: Kryptographie stellt zwar eine *notwendige*, aber eben keine *hinreichende* Bedingung zur vertraulichen und privaten Kommunikation dar. Mit gezielten Mitteln sind auch und gerade heute Observation, Prävention, Untersuchung und Abhörung möglich. Unterschieden werden muss dabei zwischen *data-in-motion* und *data-in-rest*: Ersteres meint Kommunikationsdaten, die sich in Bewegung befinden; letzteres sind Daten, die etwa auf Geräten gespeichert sind.[18] Damals wie heute ist ein Auslesen von *data-in-rest* zielgerichteter möglich, als dies für *data-in-motion* der Fall ist, allerdings braucht es dafür einen entsprechenden Zugang zu den Personen respektive den Geräten. In der digitalen Welt sind dies Beschlagnahmungen von Endgeräten oder die Ausnutzung von Schwachstellen in der Kommunikation. Auch Metadaten und die Analyse von digitalen Verkehrsdaten (engl. *traffic analysis*) erlauben eine Überwachung *trotz* Kryptographie.[19]

Damit sind zumindest Zweifel angebracht, dass das Going-Dark-Problem notwendigerweise zu einem Dual-Use-Charakter der Kryptographie führen muss. Aus praktischer Perspektive überwiegen die Nachteile einer Klassifizierung der Kryptographie als Dual-Use-Technologie und der daraus folgenden Konsequenzen. Exportbeschränkungen etwa sind mit Nachteilen für Unternehmen, Individuen und letztlich auch die nationale Sicherheit behaftet.[20] Unternehmen sind für eine erfolgreiche Informa-

18 Siehe Encryption Working Group. *Moving the Encryption Policy Conversation Forward*. Carnegie Endowment for International Peace, Sep. 2019. URL: https://carnegieendowment.org/files/EWG__Encryption_Policy.pdf (besucht am 15.04.2024), insbesondere S. 8 sowie S. 10.

19 Siehe zu Metadaten weiterführend vor allem Abschnitt 6.3 sowie Gasser u. a., *Don't Panic*. Siehe zur Analyse von Verkehrsdaten im militärischen Kontext auch Kahn, *The Codebreakers*, S. 7–9; zu den Möglichkeiten, trotz Kryptographie Zugriff auf Kommunikationsdaten zu erhalten, Daalen, „The right to encryption: Privacy as preventing unlawful access", S. 4; zur Einführung in die Möglichkeiten der Metadaten auch Anderson, *Security Engineering*, S. 781–783 sowie S. 916–919, zur Verkehrsdatenanalyse vor allem S. 782. Ob die genannten Möglichkeiten der Strafverfolgung und Justiz ethisch gerechtfertigt sind, wird an dieser Stelle nicht weiter betrachtet. Gerade vor dem Hintergrund von Spyware und der Software *Pegasus* scheint eine solche Diskussion jedoch gesellschaftlich notwendig. Für das hier vorgestellte Argument, das spezifisch die Kryptographie als Dual-Use-Technologie diskutiert, genügt jedoch die prinzipielle Möglichkeit alternativer Methoden.

20 Siehe dazu auch die Diskussion zu Exportbeschränkungen in Abschnitt 4.3.

tionssicherheit auf funktionierende Kryptographie angewiesen. Einzelne haben das begründete Interesse, vertraulich sprechen zu können. Die nationale Sicherheit erfordert, dass Unternehmen und Individuen sicher kommunizieren können, um nicht zum Ziel ausländischer Institutionen zu werden.[21] Auf der anderen Seite stehen die konsequentialistischen Vorteile einer weltweit freien, sicheren und zugänglichen Kryptographie. Auch im Kontext einer konsequentialistischen Argumentation kann daher eine Dual-Use-Klassifikation argumentativ nicht sinnvoll unterstützt werden.

Unabhängig davon ist die zweite der oben aufgeworfenen Fragen zu betrachten: Falls wir (jetzt nur noch hypothetisch) annehmen, dass Kryptographie tatsächlich eine solche Dual-Use-Technologie ist oder irgendein anderer Grund zur Exportbeschränkung von Kryptographie besteht, wie lässt sich dann eine solche normative Ansicht in der Praxis umsetzen? Bei genauerer, auch historischer Betrachtung wird ersichtlich, dass der Export von Kryptographie selbst bei einer Klassifikation als Dual-Use-Technologie realistischerweise nicht in sinnvoller Weise und gezielt beschränkt werden könnte. Kryptographie ist seit der Modernen Kryptographie letztlich Mathematik, und die Verbreitung von Mathematik lässt sich höchstens nur kurzfristig unterdrücken. Früher oder später werden Algorithmen, Fachartikel und Programme Wege finden, exportiert zu werden, sei es über das Internet, klassisch als Buch oder über den persönlichen Austausch. Bereits Kapitel 4 hat dafür Beispiele im Kontext der Crypto Wars genannt: einerseits Bernsteins Algorithmus *Snuffle*, der gemeinsam mit Bürgerrechtsorganisationen die ITAR herausgefordert hatte, andererseits Phil Karn, der Bruce Schneiers *Applied Cryptography* inklusive abgedrucktem DES-Code in Buchform exportieren durfte – DES auf einer Diskette allerdings nicht. Beide Fälle zeigen die Widersprüchlichkeiten von Exportbeschränkungen im Bereich der Kryptographie.[22]

Hinzu kommt ein zweites Argument im Kontext der Modernen Kryptographie: Kryptographie ist inzwischen eine globale Sache. Sie lebt vom internationalen Austausch der *Codemakers* und *Codebreakers*, also jener, die Algorithmen entwickeln, und jener, die sie brechen wollen. Seit Kerckhoffs steht für die Wissenschaft der Kryptographie unzweifelhaft

21 Siehe zur Kryptographie im Kontext der nationalen Sicherheit z. B. Landau, „The National-Security Needs for Ubiquitous Encryption".

22 Zu Bernstein siehe umfassend Jarvis, *Crypto Wars*, S. 238–257, zu Karn einführend Greenberg, *This Machine Kills Secrets*, S. 86–87; weiterführend Abschnitt 4.3.

fest, dass die Sicherheit des Kryptosystems *ausschließlich* in der Geheimhaltung des Schlüssels liegen darf, nicht in der Geheimhaltung des Systems.[23] Exportbeschränkungen im Sinne einer Dual-Use-Technologie widersprechen diesem Gedanken. Solche Beschränkungen führen dazu, dass auch die eigenen Algorithmen weniger überprüft werden. Konsequenterweise sinkt damit die digitale Sicherheit für alle. Aljifri und Sánchez Navarro fassten die Erfolgsaussichten von Regulierungen der Kryptographie im internationalen und globalen Kontext bereits im Jahr 2003 wie folgt zusammen:

> even if future events prompt legislators throughout the globe to once again consider stronger encryption laws or the deployment of key escrow systems, the probabilities of such undertakings to succeed will surely be very slim, due to the increasing role that cryptography has in the world today as a fundamental tool in electronic commerce, telecommunications, finances and countless other businesses and industries for which secure communications and storage are essential.[24]

Für die ethische Diskussion bedeutet dies, dass Kryptographie zur vertraulichen Kommunikation nicht nur *keine* explizite militärische Dual-Use-Technologie ist, sondern dass ihr Export und ihre Weitergabe eben auch nicht auf *einfachem* Wege beschränkt oder reguliert werden kann. Eine komplexere Regulierung etwa mit spezifischen Intermediären könnte den Export und die Nutzung von Verschlüsselungstechnologien zwar erschweren. Eine solche Regulierung würde aber, wie die kommenden Kapitel zeigen werden, zu anderen Problemen, Nebeneffekten oder Ungleichheiten führen.

Bei einer utilitaristischen Perspektive ist auch eine methodologische Kritik am Dual-Use-Gedanken im Speziellen und am Konsequentialismus im Allgemeinen zu erwähnen. So stellt sich die Frage, ob sich die positiven Folgen der Kryptographie mit ihren negativen, unerwünschten Folgen vergleichen lassen. Ist das Ausmaß der Nutzung von Kryptographie in Autokratien so groß, dass Exportbeschränkungen geboten sind? Sind die Fälle, in denen verschlüsselte Kommunikation eine Gefahr für die nationale Sicherheit darstellt, von größerem Gewicht und häufiger als die positiven Folgen ihrer Anwendung? Eine kalkulatorische Quantifizie-

23 Siehe zu Kerckhoffs' Prinzip Katz und Lindell, *Introduction to Modern Cryptography*, S. 7–8, sowie Abschnitt 1.1.

24 Aljifri und Sánchez Navarro, „International legal aspects of cryptography", S. 203.

rung ist hier nicht möglich. Sie würde zu sehr auf einem arithmetischen Verständnis von *gutem* und *schlechtem* Einsatz von Kryptographie basieren. Die hier betrachtete Dichotomie lässt sich nicht mit mathematischen Summenberechnungen auflösen. Daher stellt ein allzu starker Fokus auf solche Dual-Use-Qualifikationen eine Verkürzung für die Ethik der Kryptographie dar.

Die Beschäftigung mit der Frage nach dem *Nutzen* der Kryptographie erfordert allerdings aus einem wichtigen Grund eine weitere Perspektive. So haben sich die Argumente bisher implizit mit Kryptographie *zum Zwecke der Vertraulichkeit* auseinandergesetzt. Wie Kapitel 2 gezeigt hat, ist Moderne Kryptographie aber mehr als nur Vertraulichkeit. Sie wird auch im Rahmen von Authentizität, Nicht-Abstreitbarkeit und Zurechenbarkeit eingesetzt – alles Schutzziele, die insbesondere im Kontext der Identifikation wichtig sind. Mit diesem Wissen braucht es eine zusätzliche Perspektive, die sowohl während der Crypto Wars als auch in den vergangenen Jahren zu wenig beachtet wurde. Kryptographie zum Zwecke der Vertraulichkeit war immer wieder Teil von Regulierungsversuchen und Beschränkungen. Kryptographie mit Blick auf Authentizität und Identifikation steht hingegen selten im Rampenlicht politischer Auseinandersetzungen. Dieser Thematik ist daher ein eigener Abschnitt 7.3 zu widmen. Zuvor wenden wir uns jedoch einem Thema zu, das unterschwellig immer wieder in Diskussionen um den richtigen Umgang mit Verschlüsselung erkennbar ist: die *Privacy-vs.-Sicherheit*-Dichotomie.

6.2 Privacy vs. Sicherheit

Mit der *Privacy-vs.-Sicherheit*-Dichotomie wird eine Ansicht beschrieben, der zufolge Privacy im Konflikt mit der Sicherheit steht.[25] Auch in diesem Abschnitt wird, ähnlich wie zuvor in Abschnitt 5.2 diskutiert, der englische Begriff *Privacy* verwendet, um Problematiken in der Übersetzung

25 Siehe zur Einführung Sophie Stalla-Bourdillon, Joshua Phillips und Mark D. Ryan. *Privacy vs. Security*. London u. a.: Springer, 2014; James Bret Michael, Richard Kuhn und Jeffrey Voas. „Security or Privacy: Can You Have Both?" In: *Computer* 53.9 (2020), S. 20–30; sowie George Hurlburt u. a. „Security or Privacy? A Matter of Perspective". In: *Computer* 47.11 (2014), S. 94–98. Im Kontext von Biometrik siehe Lauren D. Adkins. „Biometrics: Weighing Convenience and National Security against Your Privacy". In: *Michigan Telecommunications and Technology Law Review* 13.2 (2007), S. 541–555.

im Deutschen zu umgehen.[26] *Sicherheit* ist außerdem nicht im Sinne des englischen Begriffs *Safety* zu verstehen, sondern primär als *Security*, wie etwa bei *National Security*, öffentlicher Sicherheit oder im Kontext des Schutzes vor Kriminalität. Vor allem während der Crypto Wars gab es eine solche „security *vs.* privacy dimension"[27], wie sie Jarvis erkennt. Im Licht der Snowden-Leaks und der Kritik an der NSA benannte auch Barack Obama, damaliger Präsident der USA, eine solche Dichotomie:

> I think it's important to recognize that you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience. We're going to have to make some choices as a society.[28]

Dieser Dichotomie liegt das Argument zugrunde, dass Privacy und Sicherheit in der ein oder anderen Form in Opposition zueinander stünden.[29] Mehr Privacy bedeute weniger Sicherheit; mehr Sicherheit bedeute weniger Privacy. Privacy und Sicherheit verhielten sich also umgekehrt proportional zueinander. Privacy werde dabei oft als ein diffuses, wenig spezifisches, bisweilen subjektives Konzept konnotiert. Sicherheit hingegen wirke indiskutabel, objektiv und immer wünschenswert. Niemand

26 *Privacy* wird hier verwendet im Sinne der Taxonomie von Solove, „A Taxonomy of Privacy". Siehe auch Abschnitt 5.2.

27 Jarvis, *Crypto Wars*, S. 5, kursiv im Original. Dabei spricht sich Jarvis für eine kompromissbereite Lösung dieser Dimension aus: „a wider perspective, that of overall digital risk to states and citizens, is required for a more comprehensive and useful framing of the government-citizen relationship and digital age civil rights provisions"; ebd., S. 5.

28 The White House Office of the Press Secretary. „Statement by the President". San Jose, CA, 7. Juni 2013. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president (besucht am 15.04.2024); teilweise zitiert in Jarvis, *Crypto Wars*, S. 321. Obama führt dann im Versuch der Verteidigung der NSA-Programme weiter aus: „And what I can say is that in evaluating these programs, they make a difference in our capacity to anticipate and prevent possible terrorist activity. And the fact that they're under very strict supervision by all three branches of government and that they do not involve listening to people's phone calls, do not involve reading the emails of U.S. citizens or U.S. residents absent further action by a federal court that is entirely consistent with what we would do, for example, in a criminal investigation – I think on balance, we have established a process and a procedure that the American people should feel comfortable about." The White House Office of the Press Secretary, „Statement by the President".

29 Phillip Rogaway bezeichnet solche Narrative auch als *law-enforcement framing*. Siehe Rogaway, *The Moral Character of Cryptographic Work*, S. 25–26.

wolle gerne auf Sicherheit verzichten, aber auf ein wenig Privacy hingegen müsse jeder verzichten können. Der Jurist Shaun B. Spencer hat diese Art der Dichotomie bereits 2002 beschrieben:

> The debate is often framed, either implicitly or explicitly, as a balancing of the tangible harms that a security proposal would prevent, against the intangible harms that an intrusion on privacy would cause. This approach presents the choice between, for example, the disastrous effects of a terrorist airline hijacking, and the relatively minor feeling of discomfort that might flow from presenting a national ID card before the boarding. Given those limited choices, what right-thinking person would not choose the latter?[30]

Für Spencer bedeutet dies eine Art „tangible-vs-intangible decision making framework"[31]. Er führt drei Argumente an, warum dieses Framework allerdings Sicherheit über- und Privacy unterbewertet: (1) Das Framework sei unvollständig, weil es viele nicht beabsichtigte Konsequenzen der Sicherheitsmaßnahmen übersehe. Die Effekte von Sicherheit seien hier lediglich kurzfristig, die Folgen für Privacy allerdings langfristig. (2) Die greifbaren Schäden oder negativen Folgen seien überbetont aufgrund einer kontextuellen Spezifität wie im Beispiel einer terroristischen Flugzeugentführung, wo sich wohl jede Person für mehr Sicherheit entscheiden dürfte. (3) Das Framework ziehe eine falsche Unterscheidung von greifbaren (engl. *tangible*) Verstößen gegen die Sicherheit und nichtgreifbaren (engl. *intangible*) Eingriffen in die Privacy. Aber auch Sicherheit sei oftmals nicht greifbar, während Eingriffe in die Privacy sehr wohl spürbare Konsequenzen für das soziale Verhalten hätten.[32]

Wenden wir diese drei Argumente nun auf den Umgang mit Verschlüsselungstechnologien an. Im Kontext der Kryptographie betrifft das erste Argument (1) das, was als *Seiten-* oder *Nebeneffekte* der Regulierung von Kryptographie beschrieben werden kann. Dies sind Konsequenzen des Handelns, die nicht das ursprüngliche Ziel des Handelns erreichen, sondern als anderweitige Effekte gelten müssen. Je nach Fall können diese Effekte lediglich Kollateralschäden sein, insofern sie vom Ziel unabhängige Folgen sind. In anderen Fällen kann es sich aber auch um Folgen handeln, bei denen das ursprüngliche Ziel konterkariert wird. Ein Beispiel

30 Spencer, „Security versus Privacy", S. 519.
31 Ebd., S. 519.
32 Siehe zu diesen drei Argumenten und diesem Absatz ebd., S. 519–520.

für Ersteres wäre, wenn durch eine Reduktion der Nutzung von Kryptographie mit dem Ziel der Sicherheit zudem das Recht auf freie Meinungsäußerung beschränkt wird. Ein Beispiel für Letzteres wäre, wenn infolge eines Verbots von Verschlüsselung die Sicherheit selbst sinkt, etwa wegen möglicher IT-Angriffe.[33]

Das zweite Argument (2) von Spencer ist ebenfalls anwendbar auf die Beschränkung und Regulierung von Kryptographie. Kontextuell sehr spezifische Beispiele führen zu einem Überbetonen von Sicherheit.[34] So würden wohl die meisten Menschen der folgenden, normativ stark wertenden und kontextuell spezifischen Argumentation zustimmen:

> *Mit der Kryptographie können gewaltbereite Kartelle untereinander kommunizieren, ohne dass ein legitimer staatlicher Zugriff auf die Kommunikation möglich wäre. Wenn wir nur eine „minimale" Zugriffsmöglichkeit auf die Kommunikation implementieren, dann können wir diese Kartelle zerschlagen. Der Privacy-Eingriff ist gering, weil ja lediglich die Kommunikation von Kartellen analysiert werden soll.*

Es fällt emotional schwer, eine solche Idee abzulehnen. Der kontextuelle Rahmen des Arguments erzeugt den gefühlten Drang nach mehr Sicherheit, insofern die meisten Menschen gewaltbereite Kartelle ablehnen dürften.[35] Gleichwohl wird durch diesen spezifischen Kontext das Ziel der Sicherheit überbetont und dadurch die (langfristige) Bedeutung von Privacy minimiert. Solche kontextuell sehr spezifischen Beispiele, die für Eingriffe in die Privacy *aller* sprechen sollen, lassen sich überraschend oft in die sogenannten *Four Horsemen of the Infocalypse* kategorisieren:

---

33 Wir können uns hierbei zur Vereinfachung ein Krankenhaus vorstellen, das aufgrund überschießender Regularien in bestimmten Bereichen der Kommunikation auf eine Ende-zu-Ende-Verschlüsselung verzichten muss. Dadurch erhöht sich die Wahrscheinlichkeit, dass ein böswilliger Hackerangriff über diese neue Schwachstelle stattfindet. Dieses Beispiel ist hier allerdings nur zur Anschauung gedacht. Ähnlich wie in Spencers Ausführungen beschrieben, sind Beispiele immer greifbar und sollten deswegen nicht als alleiniges Argument für oder gegen etwas gelten.

34 Im Kontext des Terrorismus wäre ein Beispiel hierfür der Disput zwischen Apple und dem FBI im San-Bernardino-Fall. Siehe einführend Bauer, *Secret History*, S. 521–528.

35 Eine Diskussion über *Blood, Death and Privacy* findet sich auch bei Solove, der schreibt: „Privacy is not a horror movie, most privacy problems don't result in dead bodies, and demanding more palpable harms will be difficult in many cases." Daniel J. Solove. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven und London: Yale Univeristy Press, 2011, S. 30, zum Kontext auch S. 29–31.

Drogen, Geldwäsche, Terrorismus und Pädophilie.[36] Diese provokante Darstellung geht zurück auf Tim Mays *Cyphernomicon*, in dem er auf die Frage, wie Privacy und Anonymität bekämpft werden wird, unter anderem antwortet: „like so many other 'computer hacker' items, as a tool for the 'Four Horsemen': drug-dealers, money-launderers, terrorists, and pedophiles"[37].

Auch das dritte Argument (3) ist im Kontext der Kryptographie überzeugend. Sicherheit wird rhetorisch und implizit oft als greifbar, nahbar oder definierbar angenommen. Privacy auf der anderen Seite sei diffus, subjektiv und wenig zu fassen. Tatsächlich ist aber gerade Privacy im Sinne der Vertraulichkeit ein sehr konkretes Schutzziel der Informationssicherheit.[38] Sicherheit hingegen wägt oftmals Zielkonflikte ab. Wenn Sicherheit mit dem Gefühl der Angst verbunden wird, dann handelt es sich überdies um ein subjektives und wenig fassbares Konzept.[39]

Wegen solcher Argumente ist diese Dichotomie auch relevant im Kontext der sogenannten nationalen Sicherheit.[40] Nach Diffie und Landau steht etwa fest: „Protecting the national security and enforcing the laws are basic societal values. Often they stand in competition with another basic value: privacy."[41] Doch wenn mit dem Begriff *Sicherheit* umfassender auch die digitale *Informationssicherheit* inkludiert ist, wird mit Blick auf die oben angeführten Argumente ersichtlich, dass im Kontext der nationalen Sicherheit *auch* Privacy wünschenswert ist. Privacy ist sowohl Bedingung als auch Konsequenz von digitaler Sicherheit und Vertraulichkeit. Umgekehrt bedeutet dies, dass eine Schwächung der ver-

36 Siehe z. B. Assange u. a., *Cypherpunks*, S. 69–71; diskutiert auch in Jordan, *Information Politics*, S. 104–105, sowie in Borsook, *Cyberselfish*, S. 80.

37 May, *The Cyphernomicon*.

38 Siehe zu Privacy Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 3–4.

39 Wie Spencer schreibt: „security proposals serve largely intangible goals, such as allaying people's fears." Spencer, „Security versus Privacy", S. 520.

40 Einführend zu nationaler Sicherheit siehe Marouf Hasian Jr., Sean Lawson und Megan D. McFarlane. *The Rhetorical Invention of America's National Security State*. Lanham u. a.: Lexington Books, 2015; Armand Mattelart. *The Globalization of Surveillance: The Origin of the Securitarian Order*. Cambridge und Malden: Polity Press, 2010, S. 49–78; sowie John Allen Williams, Stephen J. Cimbala und Sam C. Sarkesian. *US National Security: Policymakers, Processes, and Politics*. 6. Aufl. Boulder und London: Lynne Rienner Publishers, 2022.

41 Diffie und Landau, *Privacy on the Line*, S. 141.

traulichen Kommunikation (etwa aufgrund einer Backdoor) dazu führt, dass die digitale Sicherheit *aller* sinkt.[42]

Kryptographie ist zumindest aus der Perspektive der Informationssicherheit keine Gegenspielerin zur nationalen Sicherheit. Vielmehr hängen beide direkt proportional voneinander ab. Ohne Kryptographie kann es keine nationale Sicherheit geben. Kann eine Bevölkerung nicht vertraulich, sicher und integer kommunizieren, dann werden Bedrohungen und Angriffe von böswilligen inländischen und ausländischen Parteien wahrscheinlicher und erfolgreicher.[43] Wenn aber ein hohes Niveau an vertraulicher und privater Kommunikation besteht, dann sind auch internationale Überwachungs- und Spionageversuche erschwert. Allerdings können *auch* Kartelle, terroristische Vereinigungen oder Kriminelle solche niederschwelligen Verschlüsselungstechnologien nutzen. Angesichts der Möglichkeiten der Strafverfolgung, etwa mit Blick auf Metadaten oder die Ausnutzung von Schwachstellen digitaler Geräte, lässt sich jedoch ein Trade-off von nationaler Sicherheit und Privacy durchaus herstellen, wie das nächste Kapitel aufzeigen wird. Die Folgen für eine Gesellschaft, in der eine sichere und vertrauliche Kommunikation unterdrückt wird, sind hingegen zu schwerwiegend und zudem von Nachteil für die nationale Sicherheit. Diffie und Landau erkennen daher trotz dieses scheinbaren Konflikts von verschlüsselter Kommunikation und nationaler Sicherheit, dass „the national-security establishment decided that the widespread use of strong encryption, difficult though it make certain aspects of intelligence, was, in the end, ultimately in the nation's interest."[44]

Neben solchen konsequentialistischen Aspekten sind im Kontext einer Privacy-vs.-Sicherheit-Dichotomie zudem rhetorische (Schein-)Argumente zu identifizieren. Einerseits wollen diese Argumente zeigen, dass

42 Hinzu kommt, dass Privacy nicht nur ein individuelles Recht ist, sondern vielmehr ein sozial-gesellschaftlicher Wert; siehe Solove, *Nothing to Hide*, S. 47–52. Trotzdem sollten Privacy und Sicherheit als getrennte Konzepte behandelt werden. Bambauer erkennt dabei im Vergleich: „Privacy discourse involves difficult normative decisions about competing claims to legitimate access to, use of, and alteration of information. It is about selecting among different philosophies and choosing how various rights and entitlements ought to be ordered. Security implements those choices – it mediates between information and privacy selections." Derek E. Bambauer. „Privacy versus Security". In: *The Journal of Criminal Law and Criminology* 103.3 (2013), S. 667–683, hier S. 667.

43 Siehe umfassender und weiterführend zu *Cyber Threats* Clarke und Knake, *The Fith Domain*.

44 Diffie und Landau, *Privacy on the Line*, S. 9.

ein Handeln *dringend notwendig* sei, um eine bestimmte Sicherheit zu gewährleisten. Andererseits konnotieren die Argumente, dass der daraus folgende Schaden für Privacy gering sei. Im Kontext der Bekämpfung von Kartellen ist bereits weiter oben ein solches Argument vorgestellt worden. Unterschwellig möchten solche Argumente ausdrücken:

> *Wir müssen eben zur Sicherheit etwas Privatsphäre einschränken. Dieser Weg ist alternativlos. Apropos. Warum bist du dagegen? Warum hast du so Angst vor etwas weniger Privatsphäre? Hast du etwas zu verbergen? Hättest du nichts zu verbergen, müsstest du ja nichts befürchten.*

Diese Begründung, die scheinbar für Sicherheit und gegen Privacy spricht, wird auch als *Nothing-to-hide-Argument* bezeichnet. Daniel J. Solove, Professor an der George Washington University, stellt dieses Argument im Kontext von Privacy und Sicherheit in seinem Werk *Nothing to Hide: The False Tradeoff Between Privacy and Security* vor.[45] Beim Nothing-to-hide-Argument wird behauptet, nur diejenigen träten für Privacy ein, die auch etwas zu verbergen (engl. *to hide*) hätten. Im Umkehrschluss dürften alle, die nichts zu verbergen hätten, auch nichts dagegen haben, dass Privacy reduziert wird. In Anwendung auf die Kryptographie würde dies bedeuten, dass nur diejenigen vertrauliche Kommunikation befürworten, die ihre Kommunikation verbergen wollen – etwa, weil sie illegale Aktivitäten unter dem Deckmantel der Verschlüsselung durchführen möchten.

Allerdings greift dieses Argument zu kurz. Zunächst wäre zu fragen, ob nicht jeder Mensch etwas zu verbergen hat.[46] Das Nothing-to-hide-Argument will unterschwellig eine Schwarz-Weiß-Perspektive erzeugen, in der nur die *bad guys* etwas zu befürchten hätten, die *good guys* aber nicht. In den Worten Soloves: „But the problem with the nothing-to-hide argument is the underlying assumption that privacy is about hiding bad things“[47]. Es ist zwar unzweifelhaft, dass die *bad guys* einen Drang nach Verbergen und Geheimhaltung haben. Trotzdem ist die Annahme unbegründet, dass *ausschließlich* die *bad guys* verborgen kommunizieren

45 Siehe dazu und zum Folgenden einführend Solove, *Nothing to Hide*, insbesondere S. 21–32; dazu auch Daniel J. Solove. „‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy“. In: *San Diego Law Review* 44.1 (2007), S. 745–772. Wie häufig im Bereich der Privacy and Surveillance Studies wird dabei die Kryptographie oft nicht oder nur oberflächlich beachtet.

46 Siehe Solove, *Nothing to Hide*, S. 22–24.

47 Ebd., S. 26.

möchten. Sich mit seiner Partnerin oder seinem Partner über intime Details des Lebens auszutauschen, Gesundheitsdaten mit der Ärztin oder dem Arzt zu besprechen, eine neue Geschäftsidee zu entwickeln – all das sind Dinge, die wohl die meisten Menschen nur widerwillig der Öffentlichkeit oder jemand anderem preisgeben wollen. Zugleich sind sie aber keine illegalen Aktivitäten.

Solove erkennt aber auch, dass solche Begründungen gegen das Nothing-to-hide-Argument „the most extreme form“[48] seien. „In a less extreme form, the nothing-to-hide argument refers not to all personal information but only to the type of data the government is likely to collect.“[49] In der extremen Form bezieht sich das Nothing-to-hide-Argument also auf *alle* persönlichen Daten, in der abgeschwächten Variante nur auf jene, die für Regierungen von Interesse sind. Diese abgeschwächte Version tritt zum Beispiel im Kontext von Videoüberwachung auf, bei der schließlich das Bild relevant ist – und nicht etwa Gesundheitsdaten. Im Bereich der Kryptographie hingegen gibt es eine solche abgeschwächte Variante nicht. Aus technischer Sicht ist es nicht möglich, *nur ein gewisses Maß an* Kryptographie zu erlauben. Selbst die neuesten Versuche (namentlich das sogenannte *Client-Side-Scannning*, siehe Abschnitt 8.1) scheitern, einen Trade-off von Privacy und Sicherheit zu erreichen, sinkt doch, wie bereits mehrfach diskutiert worden ist, mit einer beschränkten und unsicheren Kryptographie auch die digitale Sicherheit. Auch wenn wir meinen, nichts vor den nationalen Strafverfolgungsbehörden verbergen zu müssen (und es ihnen z. B. zugestehen, Zugriff auf eine Backdoor zu erhalten), so gilt das sicherlich nicht für ausländische Hackergruppen, die unsere Daten verkaufen oder nutzen werden (z. B. zum Identitätsdiebstahl).

Hinzu kommt, dass das Nothing-to-hide-Argument stark vom aktuellen politischen System abhängt. Was passiert, wenn sich die rechtlichen Rahmenbedingungen ändern? Wenn das, was heute noch legal und nicht zu verbergen ist, morgen als problematisch gelten wird und nun doch verborgen werden sollte? Aus pflichtethischer Perspektive wäre dann zu fragen, ob dem Argument nicht ursächlich ein deontologischer Widerspruch im Wollen zugrunde liegt, wie er in Abschnitt 5.1 diskutiert worden ist. Jemand, der vielleicht im Heute nichts zu verbergen hat, müsste akzep-

48 Ebd., S. 24.
49 Ebd., S. 24.

tieren, dass auch im Morgen kein Verbergen von Informationen möglich sein wird.

Aber auch aus der Perspektive der Menschenrechte ist entschiedene Kritik an der Privacy-vs.-Sicherheit-Dichotomie angebracht. David Kaye, der damalige UN-Sonderberichterstatter für Meinungsfreiheit, stellt in seinem Report aus dem Jahr 2015 unmissverständlich fest:

> Discussions of encryption and anonymity have all too often focused only on their potential use for criminal purposes in times of terrorism. But emergency situations do not relieve States of the obligation to ensure respect for international human rights law.[50]

In einem Punkt haben die Verfechterinnen und Verfechter der *Privacy-vs.-Sicherheit*-Dichotomie allerdings recht: Wir können nicht beides *vollständig* erreichen, also umfassende Privacy und zugleich umfassende Sicherheit. Die Konsequenz jedoch, die sie daraus ziehen und der zufolge wir auf ein Stück Privacy verzichten müssen, ist falsch. Richtig ist vielmehr, dass es ohne Privacy keine Sicherheit geben kann. In der technologisierten Gesellschaft von heute verschwimmen digitale Sicherheit und menschliche Sicherheit. Weder öffentliche noch individuelle Sicherheit kann ohne digitale Sicherheit erreicht werden. Diese Sicherheit wird damit zur notwendigen Bedingung für eine ganzheitliche öffentliche und nationale Sicherheit. Die digitale Sicherheit setzt wiederum eine frei zugängliche und nutzbare Kryptographie voraus. Diese sowohl konsequentialistische als auch technologische und menschenrechtsbasierte Perspektive widerlegt das Nothing-to-hide-Argument und identifiziert *Privacy vs. Sicherheit* als Schein-Dichotomie.

6.3 Überwachung vs. Kryptographie

Wenn sich die *Privacy-vs.-Sicherheit*-Dichotomie nun als *Schein*-Dichotomie herausstellt und damit *nicht* gegen eine freie und zugängliche Kryptographie spricht, stellt sich weitergehend die Frage, wie in diesem Kontext Strafverfolgungsbehörden und Geheimdienste agieren können. Wenn wir es wirklich ernst meinen mit einer solchen zugänglichen Kryptographie,

50 Kaye, *A/HRC/29/32*, para. 58.

müssten wir dann nicht auch die Konsequenz ertragen, dass Behörden und Polizei keine Verbrechen per Analyse der Kommunikation aufdecken können? Wie aber könnten dann noch die Überwachung von Verbrecherinnen und Verbrechern und die Verhinderung oder Aufdeckung von Straftaten funktionieren?

Ein solcher Gedanke lässt eine weitere, unterschwellige Dichotomie erkennen: *Überwachung vs. Kryptographie*. Bei dieser Dichotomie, die sich letztlich wieder als eine Schein-Dichotomie entpuppen wird, treffen die Gegenpole von Überwachung und Kryptographie aufeinander. Die Dichotomie behauptet: Wenn eine freie und zugängliche Kryptographie möglich ist, dann ist Überwachung unmöglich. Wollen wir Überwachung, dann muss Kryptographie beschränkt werden.

Bevor das Verhältnis von Kryptographie und Überwachung näher eruiert wird, ist eine Definition des Begriffs der *Überwachung* (engl. *surveillance*) hilfreich. Craig Jarvis greift hier im Kontext der Crypto Wars auf David Lyon zurück, einen der einflussreichsten Forscher zu den sogenannten *Surveillance Studies*: *Surveillance* ist für Lyon definiert als „any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered“ [51]. Auf zwei Aspekte ist im Folgenden hinzuweisen, die diese Definition weiter spezifizieren.

Erstens spielt es insbesondere im Kontext der Kryptographie zur Definition von Überwachung keine Rolle, ob die gesammelten Daten jemanden identifizierbar machen oder ob sie zur Identifizierung genutzt werden können. Seit Jahrzehnten findet eine populäre, letztlich aber doch irreführende Diskussion über die *Anonymisierung* von Daten statt. Als Beispiel seien Gesundheitsdaten genannt: Es genügt hier nicht, lediglich Namen und Geburtsdatum zu entfernen oder zu pseudonymisieren. [52] Auch mit anderen Kennzahlen, die häufig zur Datenanalyse notwendig und daher nicht anonymisierbar sind (Alter, Geschlecht etc.), lassen sich Perso-

51 Lyon, *Surveillance society*, S. 2, zitiert in Jarvis, *Crypto Wars*, S. 3. Siehe zur Einführung in die Surveillance Studies Gary T. Marx. *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago und London: The University of Chicago Press, 2016, S. 1–39; zur Einführung in Überwachung auch Anderson, *Security Engineering*, S. 912–935.

52 Ross Anderson fasst die Probleme und Schwierigkeiten von Anonymisierungsmethoden überzeugend zusammen; siehe ebd., S. 375–376. Zur Vermeidung von Missverständnissen sei darauf hingewiesen, dass Anonymisierungstechniken trotzdem einen wichtigen Platz in Datenanalysen und in der Forschung haben.

nen und Personengruppen identifizieren. Es ist daher sinnvoll, bereits in der Definition solcher Techniken die Identifizierbarkeit auszuklammern. Gleichwohl gewinnt Überwachung eine neue Qualität, wenn *auch* Identifizierbarkeit hinzukommt. Abschnitt 7.3 wird sich dediziert mit dieser Thematik im Rahmen der Kryptographie auseinandersetzen.

Zweitens hat sich der englische Begriff *surveillance* zwar sowohl in der Alltagssprache als auch in der wissenschaftlichen Forschung im Sinne dieser Definition etabliert. Als sinnvolle Alternative würde sich aus zwei Gründen allerdings der Begriff *monitoring* anbieten: Zum einen konnotiert *monitoring* einen passiven, automatisierten Überwachungsprozess.[53] Ein solcher Prozess entspricht eher dem, was die Technologisierung der Überwachung eigentlich erst ermöglicht, verglichen mit eher zielgerichteter *surveillance*. Zum anderen *verdinglicht* der Begriff *monitoring* das zu überwachende Objekt auf sprachlicher Ebene. Dem Individuum wird Einzigartigkeit, Autonomie und Freiheit abgesprochen. Er oder sie wird zu einer Sache – einem erklärbaren Objekt, einer Maschine, einem Prozess – degradiert. Der Begriff *monitoring* spricht damit das aus, was Überwachung aus Perspektive der Überwachenden im digitalen Zeitalter ist: dauerhaftes, passives, automatisiertes Sammeln von Daten über Objekte.

Natürlich entspricht es in keiner Weise einer ethischen Grundlage, den Menschen in dieser Weise faktisch zu reduzieren. Phänomenologisch ist es allerdings eine Realität, dass eine solche Degradierung stattfindet – und wenn eine solche Degradierung stattfindet, ist eine begriffliche Spezifizierung gerade für die Ethik hilfreich. Da sich im englischen Sprachraum sowohl medial als auch wissenschaftlich der Begriff *surveillance* durchsetzen konnte, wird im Folgenden trotz der vorstehenden Erwägungen nicht auf *monitoring* zurückgegriffen. Konzeptuell aber sollte die Konnotation von *monitoring* stets im Begriff *surveillance* und *Überwachung* mitschwingen.

Diese vermeintlich klare Definition sollte auch nicht darüber hinwegtäuschen, dass Überwachung in der Realität komplex und diffus ist. In den vergangenen Jahren wurden zahlreiche Bücher und Konzepte vorgestellt, die sich aus sehr spezifischen konzeptionellen Perspektiven mit Überwachung auseinandersetzen – etwa die Idee der *Sousveillance*, bei

53 Bereits Lyon tituliert eines seiner Werke unter anderem mit „Monioring everyday life". Lyon, *Surveillance society*.

der die Überwachten die Überwachenden überwachen sollen.[54] Andere Forschung wiederum betrachtet Überwachung aus ökonomischer Perspektive, insbesondere unter dem von Shoshana Zuboff beschriebenen Konzept des *surveillance capitalism* (dt. *Überwachungskapitalismus*).[55] Wieder andere befassen sich mit dem Verhältnis von Staat und Überwachung.[56]

Kehren wir zur eigentlichen Dichotomie von *Überwachung vs. Kryptographie* zurück. John Perry Barlow, einer der Gründer der *Electronic Frontier Foundation*, hat bereits im Jahr 1995 in seinem Vorwort zu *Pretty Good Privacy* eine solche Dichotomie beschrieben:

> On one side lies a technological foundation upon which the most massive totalitarianism could be built. On the other is a jungle in which any number of anarchic guerrillas might hide, upon whom little order could ever be imposed.[57]

Auf der einen Seite steht das Modell eines Totalitarismus, das darauf aufbaut, dass Überwachungstechnologien „far more sophisticated and conducive to centralization"[58] werden. Auf der anderen Seite scheint Anarchie oder sogar Chaos zu herrschen. Die totalitäre Überwachung wird damit zur Antithese der Crypto-Anarchie. Überwachung *oder* Kryptographie ist hier das Motiv – kein Sowohl-als-auch, sondern ein Entweder-oder. Diese beiden unterschiedlichen Perspektiven – die der gesetzlosen Anarchie einerseits und der ausweglosen Massenüberwachung andererseits – bezeichnet der Kryptograph Phillip Rogaway auch als *surveillance-studies framing* respektive *law-enforcement framing*.[59]

---

54 Siehe Steve Mann. „'Sousveillance': Inverse Surveillance in Multimedia Imaging". In: *Proceedings of the 12th annual ACM international conference on multimedia*. MULTIMEDIA '04. New York, NY, USA: Association for Computing Machinery, 2004, S. 620–627. Eine radikale und interessante Form ist hier das Konzept von David Brins *The Transparent Society*; siehe David Brin. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*. Reading: Perseus Books, 1998; einführend auch Anderson, *Security Engineering*, S. 960.

55 Siehe Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

56 Siehe etwa Josh Chin und Liza Lin. *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*. New York: St. Martin's Press, 2023.

57 Barlow, *A Pretty Bad Problem: Forward to PGP User's Guide by Phil Zimmerman*; auch zitiert in Jarvis, *Crypto Wars*, S. 211.

58 Barlow, *A Pretty Bad Problem: Forward to PGP User's Guide by Phil Zimmerman*.

59 Siehe Rogaway, *The Moral Character of Cryptographic Work*, S. 25–27.

Ausgehend von der Crypto-Anarchie aus Abschnitt 3.3 könnte man den Eindruck gewinnen, dass wir durch die allgegenwärtige Kryptographie bereits im Zeitalter der Anarchie leben. Strafverfolgungsbehörden würden keine Möglichkeit mehr haben, die Inhalte von Kommunikation auszulesen, um Straftaten aufzudecken, Kriminelle zu überführen, Verbrecherinnen und Verbrecher zu verurteilen.[60] Geheimdienste, Polizei und Behörden seien dem sogenannten *Going-Dark-Problem* ausgesetzt – dem ziellosen Herumtappen im Digitalen, wo keine Möglichkeit mehr zur Ausführung und Ausübung eines staatlichen Gewaltmonopols zugelassen werde.[61] Bereits 1997 wollte der damalige FBI-Direktor Louis Freeh in einer US-amerikanischen Senatsanhörung unmissverständlich klarstellen:

> Uncrackable encryption will allow drug lords, spies, terrorists and even violent gangs to communicate about their crimes and their conspiracies with impunity. We will lose one of the few remaining vulnerabilities of the worst criminals and terrorists upon which law enforcement depends to successfully investigate and often prevent the worst crimes.[62]

Auf der anderen Seite herrscht nicht selten aber auch der Eindruck vor, dass staatliche wie unternehmerische Überwachung ubiquitär werde[63] – bis hin zu der Ansicht, dass das Gegenstück Privacy als archaisches Kon-

60 Bartlett meint zu erkennen: „The problem is […] that it's getting far more expensive and time consuming to find and prosecute online criminals, which means that the police do less and less of it." Bartlett, *The People Vs Tech*, S. 182. Für diese empirische Behauptung nennt Bartlett jedoch keine Quelle. Im Folgenden soll kritisch analysiert werden, ob die Möglichkeiten der Strafverfolgung wirklich so zeitaufwendig und teuer geworden sind, wie er behauptet. Auf der anderen Seite stehen immerhin die neuen Möglichkeiten, die die Sammlung, Aggregation und Analyse von Daten monetär und zeitlich günstiger machen.

61 Siehe zur Einführung in das Going-Dark-Problem Schulz und Hoboken, *Human rights and encryption*, S. 24–25; Gasser u. a., *Don't Panic*; sowie Traylor, „Shedding Light on the 'Going Dark' Problem and the Encryption Debate".

62 Freeh, *Statement of Louis J. Freeh, Director Federal Bureau of Investigation. Before the Senate Judiciary Committee*; auch zitiert in Greenberg, *This Machine Kills Secrets*, S. 73. Wie in diesem Kontext Tim Jordan zu Recht erkennt: „This statement is only remarkable for its failure to include paedophiles in the circle of evil that some kind of internet freedom will engender." Jordan, *Information Politics*, S. 104. Jordan verweist dabei auf die *Four Horsemen*, die bei May genannt sind. Siehe weiterführend Abschnitt 6.2.

63 Siehe einführend Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 264–270.

zept ausgedient habe. Der oder die Einzelne müsse dies nur noch akzeptieren – *the End of Privacy*.[64] Man könnte also auch von einem *Golden Age of Surveillance* sprechen, wie es Peter Swire in einer US-amerikanischen Senatsanhörung getan hat.[65] All jene digitalen Technologien scheinen ja gerade *für* den Erfolg von Strafverfolgung und Überwachung zu sprechen. Auch Diffie und Landau erkennen, dass technologische Möglichkeiten eher für die Strafverfolgung von Vorteil sind:

> It is hard to see much that microscopy, x-rays, database technology, microbiology, infrared imaging, MRI, or numerous other technologies have contributed to criminal enterprises; they have, however, given the police a host of techniques for tracking, identifying, and monitoring both people and physical objects. On balance, the impact of technology is so weighted on the side of law enforcement as to make it remarkable that crime has survived at all.[66]

Ein historisch-quantifizierbarer Vergleich mit einer Zeit *vor* der digitalen Kommunikation ist allerdings nur schwer möglich. Im Kontext der Modernen Kryptographie handelt es sich schließlich um ein neues Paradigma, das nicht mit der Zeit vor jenem Paradigmenwechsel vergleichbar ist. War es vor hundert Jahren einfacher, kriminell zu sein? War die Strafverfolgung machtloser, als sie es heute ist? Auf diese Fragen kann es kaum Antworten geben, denn sie würden eine Ordnungsrelation von zwei unterschiedlichen Paradigmen im Hinblick auf eine solche Quantität erfordern.

Isoliert betrachtet ist jedoch zu erkennen, dass *heute* die Sammlung, Speicherung und Analyse von Daten eine allgegenwärtige Realität ist.[67] Für Frank La Rue, den damaligen UN-Sonderberichterstatter für das Recht auf Meinungsfreiheit und freie Meinungsäußerung, sind es sinkende Kosten der Überwachung, die eine solche staatliche Überwachung möglich machen:

---

64 In Anspielung auf Reg Whitakers Monographie *The End of Privacy* aus dem Jahr 1999; siehe Whitaker, *The End of Privacy*.

65 Zitiert in Schulz und Hoboken, *Human rights and encryption*, S. 24; auch diskutiert in Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 268.

66 Diffie und Landau, *Privacy on the Line*, S. 137.

67 Diese Annahme soll zunächst nicht im negativen Sinne normativ-wertend sein. Die Sammlung, Speicherung und Analyse von Daten ist in vielen Fällen wünschenswert, beispielsweise im Bereich der Medizin.

> Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. As such, the State now has a greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before.[68]

Gezielte *Human Intelligence* (HUMINT) ist ökonomisch aufwendiger als *Signal Intelligence* (SIGINT) respektive *Communications Intelligence* (COMINT).[69] Bei SIGINT und COMINT ist durch eine allgegenwärtige Datenerfassung und automatische Analysen mithilfe maschinellen Lernens nur noch ein Bruchteil der Kosten zu erwarten. Während in einer Welt ohne Digitalisierung einige wenige Menschen lediglich zielgerichtet zu hohen Kosten überwacht werden konnten, kann dies nun für ganze Bevölkerungen bei geringem Aufwand geschehen.[70] Auch Craig Jarvis verdeutlicht in seiner historischen Analyse der Crypto Wars, was Massenüberwachung in dieser Art erst möglich macht:

> The historic ability of governments to develop mass surveillance capabilities has been limited by the vast labor requirements, which are economically infeasible in democratic societies. Digital technologies removed this labor constraint.[71]

Interessant ist bei Jarvis vor allem der Fokus auf demokratische Gesellschaften. Eine demokratische Gesellschaft würde es wohl kaum erlauben, einen aufwendigen und kostenintensiven Sicherheitsapparat zur Überwachung zu betreiben (eine undemokratische Gesellschaft ohne Mitbestimmung hätte hier wohl kaum eine andere Wahl). Gleichwohl scheint es, dass die Gefahr der Überwachung indessen *auch* in der Demokratie steigt, insofern Kosten und Aufwand sinken. Eine Demokratie schützt schließlich nicht *per se* vor anlassloser und automatisierter Überwachung. Dies

68 Frank La Rue. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/23/40. Human Rights Council, 2013, S. 10.

69 Zu einer Einführung siehe Diffie und Landau, *Privacy on the Line*, S. 88–95. Im Deutschen ist Human Intelligence etwas sperrig mit *menschliche Aufklärung* zu übersetzen, Signal Intelligence dagegen mit *elektronische Aufklärung*.

70 Jarvis pointiert diese Verschiebung, indem er anfügt, dass „a relatively small number of government employees can now surveil an entire citizenry"; Jarvis, *Crypto Wars*, S. 1.

71 Ebd., S. xi; siehe auch S. 1 sowie S. 3.

gilt im Besonderen dann, wenn Überwachung verschleiert wird oder über Intermediäre erfolgt.[72]

Normativ betrachtet werden – auch in liberal-demokratischen Staaten – bei der Befürwortung von Überwachung und einer Beschränkung von Kryptographie meist zwei Oberkategorien genannt: einerseits die nationale Sicherheit und andererseits die Strafverfolgung.[73] Ersteres meint häufig Themen wie Einflüsse von außerhalb des Staates, Terrorismusbekämpfung oder Verteidigung im Rahmen von Geheimdienstaktivitäten. Das Argument der nationalen Sicherheit ist historisch jedoch immer wieder missbräuchlich genutzt worden, so etwa von den US-amerikanischen Präsidenten J. F. Kennedy und Lyndon B. Johnson, vor allem aber von Richard M. Nixon im Kontext der Überwachung von Daniel Ellsberg und des *Watergate-Skandals*.[74] Die Gründe aus Sicht der Strafverfolgung hingegen beziehen sich meist eher auf *innere* Themen wie Kriminalität, Schutz von Minderjährigen oder Drogendelikte. Diese strikte Trennung von nationaler Sicherheit und Strafverfolgung, wie sie vor Jahrzehnten vielleicht noch sinnvoll war, ist heute aber nicht mehr aufrechtzuerhalten.[75] Spätestens die Snowden-Leaks haben gezeigt, dass die Grenzen zwischen nationaler Sicherheit, Strafverfolgung und Überwachung in der Realität zunehmend verschwimmen – zumindest aus Perspektive US-amerikanischer Geheimdienste.

Aus ethischer Perspektive ist zunächst konsequentialistisch zu fragen, wann Überwachung *vorteilhaft* oder *zweckdienlich* ist, insbesondere im Verhältnis zur Kryptographie. Wenn wir dabei zunächst alltägliche Situationen betrachten, fällt auf, dass gewisse Arten von Überwachung auch ohne das Argument der nationalen Sicherheit durchaus akzeptiert sind: so etwa die Kontrolle von Fahrscheinen im öffentlichen Verkehr, das Vorzeigen eines Ausweises bei Behördengängen oder auch das Monitoring eines Bibliotheksbestandes. Um den Einsatz von Überwachungskameras oder die Vorratsdatenspeicherung von IP-Adressen wird hingegen seit einigen Jahren im politischen Diskurs gestritten.

72 Siehe dazu auch Abschnitt 8.2.

73 Siehe Diffie und Landau, *Privacy on the Line*, S. 6, umfassender S. 87–140. Zur nationalen Sicherheit siehe auch Abschnitt 6.2.

74 Siehe dazu die überzeugende Argumentation in ebd., S. 195–197.

75 Für umfassende Beispiele siehe ebd., S. 137–140. Siehe auch die Diskussion bei Solove, *Nothing to Hide*, S. 62–70.

Die letztgenannte Art der Überwachung, die durch den geringen Aufwand auch zur *Massen*-Überwachung werden kann, wird vielfach aus der Perspektive der Privatsphäre und Privacy diskutiert. Interessanterweise beschäftigen sich die Surveillance Studies aber auffallend wenig mit Kryptographie. Wer sich von den akademischen Werken der Surveillance Studies eine dedizierte Auseinandersetzung mit Verschlüsselungstechnologien erhofft, wird nicht selten enttäuscht werden.[76] Die Cypherpunks hatten aber durchaus recht, dass Kryptographie und vertrauliche Kommunikation *eine* Antwort auf Überwachung sein kann, die das Individuum vor übergriffigen Staaten und Unternehmen schützen soll.[77]

Bedeutet diese Möglichkeit aber auch, dass FBI-Direktor Freeh mit dem Going-Dark-Problem recht hatte? In der Diskussion kommt oftmals zu kurz, dass Kryptographie *alleine* nicht genügt – weder zum Schutz vor Überwachung noch zum Erreichen völliger Anonymität. Hier ist auf einen entscheidenden Aspekt hinzuweisen: Die Prozesse und Systeme, die Kryptographie implementieren, ermöglichen, beschränken oder unterdrücken, sind weitaus komplexer, als es der mathematisch klare Algorithmus vermuten lässt. Zwar können wir mit hoher Sicherheit davon ausgehen, dass heutige kryptographische Algorithmen (z. B. AES) mathematisch ausreichend sicher sind, es kommen aber Umgebungsfaktoren hinzu, die diese Sicherheit in der Praxis reduzieren können. Als Beispiel sei eine Implementierung genannt, die sogenannte Seitenkanalangriffe zum Auslesen der Schlüssel ermöglicht.[78] Oder aber ein regulatorischer Rahmen, der

76 So etwa im *Routledge Handbook of Surveillance Studies*, siehe Kristie Ball, Kevin D. Haggerty und David Lyon, Hrsg. *Routledge Handbook of Surveillance Studies*. London und New York: Routledge, 2014; oder auch bei David Lyon. *Surveillance Studies: An Overview*. Cambridge und Malden: Polity Press, 2008. Eine positive Ausnahme ist hier Whitaker, *The End of Privacy*. Interessanterweise ist jedoch umgekehrt in der Forschung, die aus der Perspektive der Kryptographie oder der Informationssicherheit verfasst ist, die politisch-ethische Thematik der Überwachung oft präsent; siehe z. B. Jarvis, *Crypto Wars*, sowie Susan Landau. *Surveillance or Security: The Risks Posed by New Wiretapping Technologies*. Cambridge, MA, und London: MIT Press, 2010; darüber hinaus auch Diffie und Landau, *Privacy on the Line*.

77 Jarvis formuliert dazu prägnant: „Whether the Internet would remain free of government monitoring or would become more surveilled than the off-line world, would be determined to a significant degree by citizens' access to encryption." Jarvis, *Crypto Wars*, S. 5.

78 Siehe einführend Desmedt, „What is the Future of Cryptography?", S. 113–114. Zu Schwachstellen der Implementierung siehe auch Anderson, *Security Engineering*, S. 202–203.

dazu führt, dass ein signifikanter Teil der Bevölkerung zu geringe Schlüssellängen nutzt.[79] Eine zu geringe Nutzbarkeit (engl. *usability*) kann dazu führen, dass technisch wenig versierte Personen nicht auf sichere Kommunikationsmittel zurückgreifen.[80] Nutzende können aber auch *freiwillig* auf eine lokale Verschlüsselung verzichten, weil sie eine Art *Schlüsselwiederherstellung* (*key recovery*) möchten, die den Schlüssel in einer zentralisierten Cloud von Unternehmen speichert.[81] Spionagesoftware wie etwa *Pegasus* stellt eine weitere, ethisch jedoch kritisierbare Methode dar, die Kommunikation von Personen abzuhören.[82] Auch van Daalen weist auf solche Eigenschaften hin, welche die Verschlüsselung umgehen können:

> [T]he algorithm can be badly designed and vulnerable to attacks, the keys can be stored in a way which makes them easily discovered, or the software implementation contains a bug, which allows for circumvention of the encryption. All this means that parts of the system other than the encryption technology can also be exploited to gain access to encrypted information, something which probably explains why governments continue to gain access to unencrypted information, even though encryption is becoming increasingly common.[83]

79 Siehe hierzu die Geschichte zu DES in Abschnitt 2.2.

80 In diesem Kontext ist vor allem der Aspekt der Ungleichheit relevant, der in Abschnitt 7.2 diskutiert wird.

81 Siehe zum Verhältnis von *key recovery* und *key escrow* Diffie und Landau, *Privacy on the Line*, S. 241.

82 Zu Pegasus siehe Laurent Richard und Sandrine Rigaud. *Pegasus: The Story of the World's Most Dangerous Spyware*. New York: Henry Holt and Co., 2023. Hinzu kommt, dass ein *direkter* Zugriff auf Endgeräte weitaus erfolgversprechendere Möglichkeiten zur Ausnutzung von Schwachstellen und zur Entschlüsselung bietet. Besondere Aufmerksamkeit verdient hier der Konflikt zwischen dem FBI und Apple im Kontext des Anschlags in San Bernardino. Siehe einführend Anderson, *Security Engineering*, S. 933, sowie Bauer, *Secret History*, S. 521–528.

83 Daalen, „The right to encryption: Privacy as preventing unlawful access", S. 4. Um es mit den Worten von Diffie und Landau auszudrücken: „Equating unbreakable cryptography with the security of communications is like equating cryptanalysis with signals intelligence." Diffie und Landau, *Privacy on the Line*, S. 105. Zu den oben angeführten und weiteren Argumenten, warum das Going-Dark-Problem die Situation nicht umfassend beschreibt, siehe auch Gasser u. a., *Don't Panic*, sowie Koops und Kosta, „Looking for Some Light Through the Lens of 'Cryptowar' History". Für Gasser et al. gibt es drei Gründe: „First, many companies' business models rely on access to user data. Second, products are increasingly being offered as services, and architectures have become more centralized through cloud computing and data centers. A service, which entails an ongoing relationship between vendor and user, lends itself much more to monitoring and control than a product, where a technology is purcha-

Und auch wenn wir einmal davon ausgehen, dass die *Inhalte* der Kommunikation tatsächlich erfolgreich verschlüsselt sind und somit das Schutzziel der Vertraulichkeit auch in der Praxis erfüllt ist, sind sogenannte *Metadaten* (engl. *metadata*) von dieser Vertraulichkeit nicht per se betroffen.[84] Etymologisch handelt es sich bei diesem Begriff um die Verbindung von *meta* (dt. *über*) und *data* (dt. *Daten*). Man könnte daher sagen, dass es sich um *Daten über Daten* handelt.[85] Damit sind keine *inhaltlichen* Daten gemeint, sondern Daten, die ein zusätzlicher Teil zur erfolgreichen Kommunikation sind, wie etwa IP-Adressen oder Zeitangaben. Richard Gartner schreibt über die Funktion der Metadaten im Kontext sozialer Medien:

> From it we can tell where its author is located, how many followers, friends and favourites they have and when they opened their account; we can also read a description of themselves that they added to their Twitter profile. Obviously there's more to metadata than „transactional" information alone.[86]

Viele der alltäglichen Anwendungen wie etwa Messengerdienste verarbeiten zur korrekten Funktionsweise Metadaten. Mit wem wir schreiben, wann wir schreiben, wie oft wir schreiben – all das ist für die Betreiber dieser Dienste weiterhin ersichtlich. Übliche Messengerdienste verschlüsseln damit zwar den Inhalt der Kommunikation (Beispiel: „Treffen wir uns morgen im Park?"), nicht jedoch die damit verbundenen Metadaten (Beispiel: Gesendete Textnachricht am 2. Januar 2021 um 14:23, gesendet an den Kontakt mit dem Namen „Schwester"). Auch wenn also eine Ende-zu-Ende-Verschlüsselung für die Inhalte der Kommunikation implementiert werden, schützt dies nicht vor einer Überwachung der Metadaten.

---

sed once and then used without further vendor interaction. Finally, the Internet of Things promises a new frontier for networking objects, machines, and environments in ways that we just beginning to understand." Gasser u. a., *Don't Panic*, S. 10.

84 Siehe in diesem Kontext zu Metadaten Schulz und Hoboken, *Human rights and encryption*, S. 22–23, außerdem Gasser u. a., *Don't Panic*, S. 3, sowie Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 268–270. Zur Einführung in Metadaten und Verkehrsdatenanalyse siehe auch Anderson, *Security Engineering*, S. 781–783 sowie S. 916–919; zu Metadaten im Kontext von Snowden und der NSA Greenwald, *No Place to Hide*, S. 199.

85 Pomerantz definiert den Begriff wie folgt: „the word 'metadata' indicates something that is beyond the data: a statement or statements about the data." Pomerantz, *Metadata*, S. 6.

86 Gartner, *Metadata*, S. 1–2.

Auch Gasser u. a. erkennen in ihrem Report zum Going-Dark-Problem, dass Metadaten oft nicht verschlüsselt sind und dies wohl auch so bleiben dürfte:

> Metadata is not encrypted, and the vast majority is likely to remain so. This is data that needs to stay unencrypted in order for the systems to operate: location data from cell phones and other devices, telephone calling records, header information in e-mail, and so on. This information provides an enormous amount of surveillance data that was unavailable before these systems became widespread.[87]

Zwar gibt es Methoden, die mithilfe kryptographischer Verfahren *auch* Metadaten verschleiern. Das bekannteste Beispiel dürfte das *Tor-Projekt* sein, das auf dem Onion Routing basiert.[88] Nachrichten werden dabei über verschiedene *Knoten* übermittelt. Die IP-Adresse und die Herkunft der Nutzerin oder des Nutzers sollen damit für die empfangende Partei unbekannt bleiben. Doch auch wenn solche Methoden zur Prävention von Metadaten-Sammlung prinzipiell zur Verfügung stehen, werden sie bislang nicht so verbreitet eingesetzt wie eine Ende-zu-Ende-Verschlüsselung der inhaltlichen Kommunikation.

Die Gründe dafür sind vielfältig. Wie das Beispiel des Onion Routings zeigt, ist der Schutz vor einer Sammlung von Metadaten nur auf komplexe und dezentrale Weise möglich. Insbesondere die Nutzbarkeit leidet oftmals unter diesen Voraussetzungen. Hinzu kommen signifikante Performance-Einbußen, die für viele einen Trade-off von Sicherheit und Bequemlichkeit erzwingen. Die Vertraulichkeit von Metadaten zu gewährleisten, stellt sich daher meist als komplexer und schwieriger heraus als die Verschlüsselung selbst. Ist es aber nicht ohnehin so, dass inhaltliche Daten schützenswerter sind als Metadaten?

Um aufzuzeigen, dass dies *nicht immer* der Fall ist, genügen einige Beispiele. Man stelle sich etwa eine Region vor, in der das Ausleben von Homosexualität hart bestraft wird. Für die Strafverfolgungsbehörden in diesem Land reicht es für einen Anfangsverdacht bereits aus, wenn eine dauerhafte und intensive Kommunikation mit spezifischen Gruppierungen, NGOs oder Interessenvereinigungen stattfindet, die Homosexualität

87 Gasser u. a., *Don't Panic*, S. 3.

88 Siehe dazu Schulz und Hoboken, *Human rights and encryption*, S. 22–23; einführend zu Tor auch Anderson, *Security Engineering*, S. 674–676; im Kontext von Lessigs *Code is Law* siehe Webb, *Coding Democracy*, S. 55.

legalisieren wollen. Oder ein anderes Beispiel: Auch wenn die Kommunikationsinhalte mit all unseren Kontakten im Messengerdienst Ende-zu-Ende-verschlüsselt sind, ist eine umfassende Profilerstellung unserer Persönlichkeit weiterhin möglich. Mit wem wir schreiben, wie oft wir schreiben; dass wir bereits mehrfach Kontakt mit einer psychologischen Beratungsstelle aufgenommen haben, nachdem eine Arbeitsstelle gekündigt wurde; dass wir in Kontakt mit einer religiösen Minderheit stehen, für die wir uns zu interessieren scheinen – all diese Informationen gestatten es, mit einer *Aggregation* der Daten ein umfassendes Profil unserer Persönlichkeit zu erstellen.[89]

Einzelne Informationen an sich sind vielleicht wenig schützenswert. Wenn allerdings viele dieser einzelnen Informationen zusammengetragen werden, entsteht ein Gesamtbild der Person.[90] Und dieses Gesamtbild kann zur Kontrolle, zur Einflussnahme oder zur Einschüchterung genutzt werden – bis hin zu körperlichen Angriffen. In einem irritierenden Moment einer für Geheimdienste ungewöhnlichen Offenheit stellte Michael Hayden, ehemaliger Direktor der NSA und der CIA, die Bedeutung von Metadaten unverblümt dar: „We kill people based on metadata."[91]

Aus ethischer Sicht ist daher auch zu fragen, ob und wie Metadaten im Sinne der Menschenrechte schützenswert sind. Wie bereits Abschnitt 5.2 eruiert hat, schützt die AEMR den Schriftverkehr vor willkürlichen Eingriffen.[92] Bedeutet dies nun, dass auch Metadaten darunter zu fassen sind? Rein vom Wortlaut her ist das vielleicht zunächst zu ver-

89 Daniel J. Solove beschreibt diese *Aggregation* im Kontext des Nothing-to-hide-Arguments; siehe Solove, *Nothing to Hide*, S. 27; siehe auch Solove, „A Taxonomy of Privacy", S. 506–511.

90 Siehe ebd., S. 507. Ross Anderson zeigt einführend auf, welche Bedeutung die algorithmische Verarbeitung im Kontext der Überwachung hat; siehe Anderson, *Security Engineering*, S. 920–921. Zur Bedeutung von Metadaten im Vergleich zu Inhaltsdaten siehe auch die Diskussion in Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 268–270.

91 Berichtet und zitiert etwa in Lee Ferran. „Ex-NSA Chief: 'We Kill People Based on Metadata'". In: *ABC News* (12. Mai 2014). URL: https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata (besucht am 15.04.2024). Man könnte annehmen, Hayden hätte diesen Einsatz in der Diskussion an der Johns Hopkins University aus dem Jahr 2014 kritisieren wollen. Ganz im Gegenteil wollte er jedoch auf eine groteske Art und Weise erklären, dass dies bei US-Amerikanerinnen und -Amerikanern nicht genutzt werde. Auch zitiert in Rogaway, *The Moral Character of Cryptographic Work*, S. 27.

92 Die EMRK kennt einen ähnlichen Artikel; siehe dazu Abschnitt 5.2.

neinen, wenn dadurch der Schriftverkehr mit dem Inhalt der Nachricht selbst gleichgesetzt wird. Gleichzeitig handelt es sich bei dieser Frage um eine *latent ambiguity*, wie sie in Anlehnung an Lawrence Lessig in Abschnitt 5.3 diskutiert worden ist: Bei der Niederschrift und der Verabschiedung der AEMR waren Metadaten weitgehend unbedeutend. Mit der heutigen Rechenleistung und der massiven Ansammlung von Metadaten ermöglichen es solche *Daten über Daten* jedoch, ein präzises Profil eines Individuums zu erstellen. Juristisch hat der Europäische Gerichtshof für Menschenrechte in Straßburg seit 1984 mehrfach anerkannt, dass auch die Verarbeitung von Metadaten einen Eingriff in die Korrespondenz darstellt.[93] Zuiderveen Borgesius und Steenbruggen schreiben mit Blick auf die Rechtsprechung:

> In sum, metadata are protected under art. 8 ECHR [European Convention on Human Rights], but when assessing an interference the ECtHR [European Court of Human Rights] works from the assumption that capturing communications metadata will normally constitute a less serious infringement than capturing communications content. To some extent, that distinction is understandable, because some metadata need to be processed by the service provider in order to provide the service.[94]

Nach dieser Ansicht wären Inhaltsdaten in der Bewertung von Metadaten zu unterscheiden. Angesichts der oben vorgenommenen Diskussion ist jedoch zu hinterfragen, ob Metadaten *per se* einen geringeren Eingriff darstellen. Zudem existiert keine *unausweichliche Notwendigkeit* einer *zentralen* Verarbeitung von Metadaten, wie an technologischen Beispielen wie Tor deutlich wird. Darauf aufbauend kann somit auch kein hinreichendes Argument für die Sammlung von Metadaten konstruiert werden. Umgekehrt wäre vielmehr zu fragen, ob aus normativer Sicht nicht eher *mehr* Möglichkeiten zur Verschleierung von Metadaten angeboten und gefördert werden sollten.

Unabhängig davon, ob wir im Rahmen von Kryptographie vs. Überwachung nun an Implementierungsfehler oder Metadaten denken: Kryptographie ist nur *ein* Werkzeug zum Schutz vor Überwachung – und um-

93 Siehe Ni Loideain, „EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era", S. 55, sowie Bernal, „Data gathering, surveillance and human rights", S. 248. Insbesondere relevant ist hier der Fall *Malone v. United Kingdom*.

94 Zuiderveen Borgesius und Steenbruggen, „The Right to Communications Confidentiality in Europe", S. 316.

gekehrt ist Überwachung *trotz* Kryptographie möglich. Verschlüsselung ist in diesem Kontext daher zwar eine *notwendige* Bedingung für den Schutz vor Überwachung, jedoch keine *hinreichende*. Ohne ubiquitäre Kryptographie wird Überwachung in jedem Fall allgegenwärtig. Ubiquitäre Kryptographie bedeutet allerdings nicht, dass Überwachung gänzlich unmöglich wird. Dieses Faktum bringt die Kryptographin Susan Landau prägnant auf den Punkt:

> There are, after all, other ways of going after communications content than providing law enforcement with "exceptional access" to encrypted communications. These include using the existing vulnerabilities present in the apps and systems of the devices themselves. While such an approach makes investigations more expensive, this approach is a tradeoff enabling the vast majority of communications to be far more secure.[95]

Ein gezielter Versuch des Auslesens oder Mithörens von Kommunikation ist offensichtlich kostspieliger und aufwendiger als eine *generelle* Überwachung. Demokratische und liberale Gesellschaften sollten sich aber fragen, wie viel es ihnen wert ist, *sowohl* Strafverfolgung *als auch* eine verschlüsselte Kommunikation zu ermöglichen. Eine kostengünstige Überwachung und zugleich die Wahrung der Privatsphäre sind nicht realisierbar. Sehr wohl machbar ist aber eine richterlich beaufsichtigte, spezifische Überwachung, die sich auf Schwachstellen in Systemen, Metadaten oder Observationen stützt. Zwar treten bei einer solchen Art der Überwachung weitere ethische Fragen auf, sie sind aber unabhängig von der Kryptographie und sollen daher an dieser Stelle nicht weiter behandelt werden. Den Ansatz einer zielgerichteten, ausgewogenen und nur im Ausnahmefall gerechtfertigten Entschlüsselung erkennt jedenfalls auch der damalige UN-Sonderberichterstatter für Meinungsfreiheit:

> Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals.[96]

95 Landau, „The National-Security Needs for Ubiquitous Encryption", S. 2.

96 Kaye, *A/HRC/29/32*, para. 60. Bei diesem Report handelt es sich um „UN's first authoritative in-depth account of the human rights status of encryption as well as anonymity", so Schulz und Hoboken, *Human rights and encryption*, S. 28.

Egal, wofür sich Gesellschaften letztlich entscheiden werden, aus ethischer und technologischer Perspektive gilt jedenfalls, dass keine *Überwachung-vs.-Kryptographie*-Dichotomie besteht. Überwachung ist möglich *trotz* Kryptographie. Kryptographie ist lediglich eine *notwendige*, jedoch keine *hinreichende* Bedingung für den Schutz der eigenen Daten. Das Going-Dark-Problem ist daher nicht überzeugend. Die einzige Dichotomie, die tatsächlich existiert, ist die der *kostengünstigen* Überwachung vs. Kryptographie.

7 Transparenz, Gleichheit und Identität

> Daher zog er sich wieder auf den Berg zurück, er allein.
> – Joh 6,15[1]

Das letzte Kapitel hat unterschiedliche (Schein-)Dichotomien diskutiert. Diesen war gemein, dass sie oftmals eine konsequentialistische oder utilitaristische Programmatik verfolgen: Zielkonflikte im Dual-Use-Sinne, Privacy vs. Sicherheit und Überwachung vs. Kryptographie. Wenn sich eine solche Dichotomie nun als Schein-Dichotomie entpuppt hat, dann lag dies nicht an einer methodologischen Kritik des Utilitarismus, sondern vielmehr an den utilitaristischen Argumenten selbst, die nicht gegen eine freie und zugängliche Kryptographie gesprochen haben.

In diesem Kapitel werden wir auf diesen Erkenntnissen aufbauen, jedoch zudem drei Kernmotive inkludieren, die die Diskussionen um den *richtigen* Umgang mit Kryptographie seit Langem begleiten: Transparenz, Gleichheit und Identität. Diese drei Themen führen das weiter, was die vorherigen Argumente bereits grundgelegt haben. Abschnitt 7.1 befasst sich mit dem Verhältnis von Transparenz, Kryptographie und dem sogenannten Whistleblowing. Abschnitt 7.2 diskutiert daraufhin Kryptographie im Kontext von Gleichheit als eine sogenannte *egalitäre Kryptographie*. Abschnitt 7.3 schließlich eröffnet ein konzeptionell neues Thema: Kryptographie, Identität und Authentifizierung.

7.1 Transparenz und Verschlüsselung

Das folgende Phänomen kann als *Ironie von Transparenz und Verschlüsselung* beschrieben werden. Ihm liegt der Gedanke zugrunde, dass Kryptographie im Sinne der Verschlüsselung das Gegenteil von Transparenz sein müsse: Die Idee von Verschlüsselung ist ja gerade das Geheimnis, das Verborgene, das Nicht-zu-Entschlüsselnde. Die folgenden Argumente werden zeigen, dass diese Analyse nicht korrekt ist, und darauf aufbauend

1 Die Bibel. Einheitsübersetzung der Heiligen Schrift. Gesamtausgabe. Stuttgart: Verlag Katholisches Bibelwerk, 2016.

ein normatives Verhältnis von Kryptographie und Transparenz entwickeln. Tatsächlich haben Transparenz und Verschlüsselung nämlich ein anderes und vor allem komplexeres Verhältnis zueinander.

Zunächst sind bereits an dieser Stelle zwei konzeptuelle Ebenen der Transparenz im Sinne der Kryptographie zu unterscheiden: Die eine beschreibt das, was kryptographische Protokolle wirklich leisten – eine Verschlüsselung zur Geheimhaltung. In diesem Sinne käme Kryptographie der Vorstellung von Intransparenz entgegen. Dies entspricht auch dem, was Teil I als *Klassische Kryptographie* bezeichnet hat. Die zweite Ebene allerdings kehrt diese erste Einschätzung ironischerweise um, indem die *Moderne Kryptographie* und dessen Entwicklung nun im Kontext betrachtet wird: Kryptographische Algorithmen sind nur dann erfolgreich, wenn sie öffentlich sind und Forschende auf der ganzen Welt am Austausch von *Codemakers* und *Codebreakers* teilnehmen können. Eine Kryptographie, die in den Hinterzimmern von Behörden, Unternehmen und Geheimdiensten entwickelt wird, kann heute nicht die Sicherheit ermöglichen, wie es bei öffentlichen Standardisierungsverfahren und Ausschreibungen der Fall ist. Deutlich wird das etwa am Vergleich von DES und AES: Die Prinzipien des Designs der S-Boxen von DES waren auf Druck der NSA nicht veröffentlicht worden.[2] Wer würde angesichts dessen der Sicherheit von DES mehr vertrauen als derjenigen von AES, dessen Designentscheidungen vollständig veröffentlicht worden waren?

Eine solche Intransparenz und Geheimhaltung der kryptographischen Verfahren war womöglich bis in die 1970er-Jahre realisierbar. Durch das Internet und die Entwicklungen der letzten fünfzig Jahre hat sich dies allerdings gewandelt. Daraus folgt, dass kryptographische Algorithmen und Designs zwangsläufig zugänglich und bekannt werden. Dies ist die natürliche Konsequenz von Kerckhoffs' Prinzip.[3] Der Status quo stellt sich heute so dar, dass nicht mehr nur Geheimdienste auf eine starke Kryptographie zurückgreifen können, sondern auch eine Bäckerin in Süddeutschland, ein Aktivist in Myanmar oder eine Lehrerin in Brasilien. Die frühere Asymmetrie kryptographischer Nutzbarkeit ist einer ubiquitären Anwendungsmöglichkeit für *alle* Menschen gewichen. Wenn aber *alle* Menschen verschlüsselt kommunizieren können, dann ist der Vorteil der ehemals monopolisierten Kryptographie von Militär, Diplo-

2 Siehe Abschnitt 2.2.

3 Siehe zu Kerckhoffs' Prinzip Abschnitt 1.1.

matie und Geheimdiensten obsolet. Das Verhältnis von Transparenz und Kryptographie hat sich durch den Paradigmenwechsel verändert.

Betrachten wir dieses Verhältnis genauer, so ist weiter zu fragen, ob das in Verbindung der beiden konzeptuellen Ebenen nicht auch bedeutet, dass die Intransparenz ubiquitär geworden ist oder in Zukunft werden wird. Wenn dem so wäre, müssten wir neu eruieren, ob Kryptographie womöglich doch *gut* oder *schlecht* ist. Die Antwort auf diese Fragen hängt davon ab, von welchem normativen Verständnis von *Intransparenz* oder *Transparenz* ausgegangen wird. Dieses Kapitel orientiert sich im Folgenden an einer Maxime, die ursprünglich auf die Cypherpunks zurückgeht: *Privacy for the weak, transparency for the powerful!*[4] Während von öffentlichen Institutionen oder Personen des öffentlichen Lebens ein möglichst hohes Maß an Transparenz eingefordert werden soll und darf, soll sich das einzelne Individuum auf das Recht auf Privacy berufen können. Wie es der Journalist und Rechtsanwalt Glenn Greenwald formuliert: „Transparency is for those who carry out public duties and exercise public power. Privacy is for everyone else."[5] Bezogen auf Privacy für die Schwachen ist diese Maxime mit Blick auf die Menschenrechte, die in Abschnitt 5.2 im Kontext der Kryptographie diskutiert worden sind, begründbar.[6] Warum aber soll Transparenz für die Mächtigen gelten?

In der Hackerethik findet sich die Idee einer freien und ungehinderten Verbreitung von Information – *all information should be free*.[7] Information ist im demokratischen Kontext eine Grundlage für faktenbasierte Diskussion, Meinungsbildung und Entscheidungsprozesse. Ohne Information kann eine Meinung nicht fundiert sein. Das Gegenteil dazu wären Staaten, Institutionen und Organisationen, die diesen Informationsfluss unterbinden. Dieses Gegenteil zur Transparenz ist damit die

4 Siehe etwa Assange u. a., *Cypherpunks*, S. 7; weiterführend zur Diskussion Melissa de Zwart. „Privacy for the weak, transparency for the powerful*". In: *Comparative Defamation and Privacy Law*. Hrsg. von Andrew T. Kenyon. Cambridge: Cambridge University Press, 2016, S. 224–245; sowie Patrick D. Anderson. „Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange". In: *Ethics and Information Technology* 23.3 (2021), S. 295–308. Siehe zudem einführend Webb, *Coding Democracy*, S. 68–70, zu Assange auch S. 51–52.

5 Greenwald, *No Place to Hide*, S. 209.

6 Siehe auch die Argumentation bei Zwart, „Privacy for the weak, transparency for the powerful*", S. 243–244.

7 Siehe Levy, *Hackers: Heros of the Computer Revolution*, S. 28–29, im Kontext von Autorität und Dezentralisierung auch S. 29–31. Zur Einführung in die Hackerethik siehe auch Webb, *Coding Democracy*, insbesondere S. 1–31.

Geheimhaltung. Greenwald, der 2013 die Snowden-Dokumente im *Guardian* veröffentlicht hat, schreibt auch: „Secrecy is the linchpin of abuse of power, we discovered, its enabling force. Transparency is the only real antidote."[8] Patrick D. Anderson fasst diese Verbindung der Cypherpunks von Privacy auf der einen und Transparenz auf der anderen Seite wie folgt zusammen:

> First, the cypherpunks argue that privacy for the weak ought to be ensured through practical action and technological engagement. Depending on the state of surveillance in a given context, such privacy may or may not be a manifest reality; regardless, the demand for such privacy is a normative commitment for the cypherpunks. Second, the cypherpunks argue that transparency for the powerful ought to be pursued through practical action and technological engagement. While governments and corporations continue to become increasingly secretive, the cypherpunks argue that citizens and publics can use technology to undermine such secrecy and force these institutions to be more open.[9]

Wenn wir von einem solchen normativen Verständnis ausgehen, ist zu fragen, wie sich die Kryptographie dazu verhält.[10] Zwei Unterkategorien lassen sich hier getrennt untersuchen: (1) Privacy von Individuen bzw. den Schwachen, (2) Transparenz der Mächtigen und öffentlicher Institutionen. Zu (1) lässt sich zunächst unzweifelhaft feststellen, dass ubiquitäre Kryptographie dem Individuum zu Privacy und Intransparenz verhilft. Zwar ist Kryptographie keine *hinreichende* Bedingung für Privacy oder Informationssicherheit, doch ist ihre Anwendung zumindest eine *notwendige* Bedingung. Dadurch, dass Individuen aufgrund von asymmetrischer Kryptographie nicht auf ein zentrales Schlüsselmanagement angewiesen sind (etwa bei Messengerdiensten), ist auch deren Vertraulichkeit ge-

8 Greenwald, *No Place to Hide*, S. 12.

9 Anderson, „Privacy for the weak, transparency for the powerful", S. 300. Anderson arbeitet in seinem Artikel heraus, wie sich Assanges Vorstellung von jener der frühen Cypherpunks unterscheidet, und fasst zusammen: „On the one hand, Assange argues that pursuing privacy for the weak through the use of cryptography does not merely prevent government intrusions into individual privacy but actually forms the basis of an open world culture. […] On the other hand, Assange argues that pursuing transparency for the powerful through the use of cryptography does not merely create information black markets but actually disrupts the conspiratorial networks hidden inside large institutions"; ebd., S. 306.

10 Auch Maureen Webb spricht sich aus der Perspektive einer Anwältin dafür aus, dass diese Vorstellung der Cypherpunks ein *demokratisches* Manifest sei; siehe Webb, *Coding Democracy*, S. 68.

wahrt. Historisch hat *Pretty Good Privacy* (PGP) gezeigt, dass eine solche Kryptographie in der Realität machbar ist. Heute existieren zahlreiche weitere Messengerdienste, deren Code quelloffen ist und die den aktuellen Stand der kryptographischen Forschung implementieren.[11]

Die bisherigen Erwägungen bezogen sich auf die *räumliche* Anwendung der Kryptographie, bei der mehrere Parteien an unterschiedlichen Orten miteinander vertraulich und sicher kommunizieren wollen. Eine Verschlüsselung findet aber auch auf der *zeitlichen* Ebene Anwendung: Daten werden beispielsweise auf einer Festplatte verschlüsselt, um selbst bei einer Beschlagnahmung des Geräts die Vertraulichkeit zu wahren.[12] Ein mit AES korrekt verschlüsselter Datenträger lässt sich ohne den zugehörigen Schlüssel weder von Strafverfolgungsbehörden noch von sonstigen Drittparteien entschlüsseln. Diese Akteure werden daher versuchen, an den Schlüssel zu gelangen. Womöglich ist er irgendwo aufgezeichnet oder notiert; womöglich handelt es sich auch um ein schwaches Passwort, das mit Brute-Force-Attacken gefunden werden kann. Als letztes, skrupelloses Mittel könnte eine Person gefoltert und zur Herausgabe des Schlüssels bzw. Passworts gezwungen werden – hier wird von *Rubber-Hose Cryptanalysis* gesprochen.[13]

Aber auch hier kann Kryptographie die Möglichkeit von Privacy für das Individuum stärken. Julian Assange entwickelte bereits ab 1997 ein Programm mit der Bezeichnung *Rubberhose*.[14] Das Ziel des Programms ist es, eine Festplatte so zu verschlüsseln, dass es mehrere Speicherorte mit mehreren Schlüsseln gibt: „if someone grabs your Rubberhose-encrypted hard drive, he or she will know there is encrypted material on

11 Das bedeutet nicht, dass diese Messenger fehlerfrei sind. Implementierungsfehler, sogenannte Side-Channel-Attacken oder komplexe Anwendungen können die Sicherheit reduzieren. Abermals ist daher zu betonen, dass die Theorie der Kryptographie die notwendige Bedingung zur sicheren Kommunikation darstellt – allein aber für diese nicht hinreichend sein kann. Siehe ausführlicher Kapitel 6.

12 Siehe zur räumlichen und zeitlichen Ebene der Verschlüsselung die Ausführungen in Abschnitt 2.4 sowie Katz und Lindell, *Introduction to Modern Cryptography*, S. 5–6.

13 Siehe Greenberg, *This Machine Kills Secrets*, S. 125–126. Auch in diesem Jahrtausend ist davon auszugehen, dass Folter ein Mittel zur Entschlüsselung darstellt, so wurde dies etwa im Iran oder in Syrien praktiziert; siehe Anderson, *Security Engineering*, S. 912.

14 Siehe Greenberg, *This Machine Kills Secrets*, S. 125–129, sowie Suelette Dreyfus. *The Idiot Savants' Guide to Rubberhose: What is Rubberhose?*. URL: https://archive.ph/20121029045140/http://marutukku.org/current/src/doc/maruguide/t1.html (besucht am 15.04.2024); einführend Webb, *Coding Democracy*, S. 52.

it, but not how much – thus allowing you to hide the existence of some of your data."[15] Die Hoffnung ist, dass eine böswillige Partei, die möglicherweise sogar Gewalt und Folter anwendet, von einer weiteren Analyse des Datenträgers absieht, da sie einige Daten lesen, weitere Daten aber nicht erkennen kann und von deren Existenz auch nichts weiß.[16] Verschlüsselung stärkt – sofern korrekt angewandt – die Möglichkeit von Privacy für das Individuum.

Was aber bedeutet eine solche Erkenntnis für die Normativität der Kryptographie? Sollte Kryptographie beschränkt, reguliert oder reduziert werden? Wir können zunächst argumentieren, dass jeder Mensch an einem bestimmten Punkt auch Privatperson ist, selbst Regierende, Popstars oder CEOs von internationalen Unternehmen. Auch wenn sie sich in einer öffentlich hervorgehobenen Position befinden, sind sie zumindest gelegentlich *auch* Privatpersonen. Kann es dann aber sinnvoll und vernünftig sein, wenn Regierende oder CEOs Kryptographie beschränken wollen, um Privatpersonen zu überwachen oder zu kontrollieren? Normativ ist zu fragen, ob es sich bei einer Beschränkung von Kryptographie nicht um einen deontologischen Widerspruch im Wollen handeln dürfte, insofern jede Person auch Privatperson ist, die auf Kryptographie angewiesen ist.

Gleichzeitig gilt es hier, um Gegenargumente zu entkräften, zu bedenken, dass es so etwas wie *nur ein bisschen* Kryptographie nicht geben kann. Mit *nur ein bisschen* Kryptographie ist gemeint, dass Kryptographie nicht *absolut* sicher und erfolgreich ist, sondern nur *relativ*. Bestimmte Institutionen wie Strafverfolgungsbehörden sollen dadurch weiterhin Zugriff erhalten können, sofern es legitime Gründe gibt. Als Beispiel kann die Diskussion um die Schlüssellänge von DES gelten, die bereits in Abschnitt 2.2 erörtert wurde. Im Kontext des Client-Side-Scannings wird sich Abschnitt 8.1 mit ähnlichen (Gegen-)Argumenten zur Ende-zu-Ende-Verschlüsselung auseinandersetzen.

15 Dreyfus, *The Idiot Savants' Guide to Rubberhose*.

16 Auch hier gibt es natürlich in der Praxis zahlreiche Fallstricke, die einen solchen *theoretischen* Erfolg verhindern können. Zum einen müssen die Daten im ersten Speicherort auch wirklich überzeugend sein – andernfalls kann eine böswillige Partei schnell vermuten, dass ein Speicherort verborgen ist. Zum anderen sind auch in diesem Fall alle praktischen Schwierigkeiten von angewandter Kryptographie zu bedenken, angefangen von Implementierungsfehlern bis hin zu allzu kurzen Passwörtern. Besonders skrupellose Parteien könnten zudem unabhängig von der Wahrscheinlichkeit eines *hidden volume* zur Folter greifen.

Entscheidend ist hier, dass der Drang nach *nur ein bisschen* Kryptographie unvernünftig ist. Kapitel 6 hat bereits gezeigt, dass aus konsequentialistischer Perspektive eine schwache Kryptographie zur Gefahr für das Individuum und die öffentliche Sicherheit werden kann. Jede Person, die trotzdem *nur ein bisschen* Kryptographie für das Individuum und die Gesellschaft möchte, wird sich rasch in einem Widerspruch der technologischen Realität wiederfinden: Entweder Kryptographie ist so sicher und so erfolgreich wie möglich, oder sie ist sinnlos. *Schwache* Kryptographie ist *keine* Kryptographie. Einen Mittelweg oder Kompromiss kann es hier nicht geben.[17]

Die Folge ist, dass nur für zwei Positionen argumentiert werden kann: (A) Wir möchten digitale, individuelle und öffentliche Sicherheit und Privacy. Dann ist eine freie und zugängliche Kryptographie die *unausweichliche* Implikation. (B) Wir verzichten auf digitale, individuelle und öffentliche Sicherheit und Privacy. In diesem Fall können wir auch Kryptographie bewusst schwächen oder deren Nutzung beschränken. Eine Kombination aus (A) und (B) ist jedoch ein Widerspruch, der nicht aufgelöst werden kann. Wenn wir also die Prämisse von (A) wollen, wovon hier ausgegangen wird, dann sind Individuen, Staaten und Unternehmen in der moralischen Pflicht, Kryptographie zumindest zuzulassen und gegebenenfalls sogar zu fördern.

Geben diese Überlegungen Aufschluss über die Normativität im Hinblick auf Privacy für die Schwachen (1), ist weiter zu fragen, wie es sich mit der Forderung nach Transparenz der Mächtigen und öffentlicher Institutionen verhält (2). Welchen Einfluss hat die Kryptographie auf diese Transparenz? Zunächst gilt auch hier wieder, dass die gleichen Methodiken der Individuen auch für die Mächtigen dieser Welt nutzbar sind. Es scheint also, dass mit Kryptographie Privacy für die Schwachen *und* für die Mächtigen erreicht werden kann. Im Vergleich zu einer Welt, in der *ausschließlich* die Mächtigen auf Intransparenz und Kryptographie zurückgreifen können, ist dies bereits ein Novum im Sinne eines neuen Paradigmas.[18]

17 Ein Vergleich mit dem Briefgeheimnis ist hier nicht möglich, insofern es sich dabei um eine *latent ambiguity* handeln würde. Siehe zu *latent ambiguities* Abschnitt 5.3.

18 So bedeutet es einerseits, dass die Autorität über die Entwicklung von Kryptographie dezentralisiert wurde. Teil I hat gezeigt, dass über die Kryptographie zunehmend an öffentlichen Universitäten geforscht wurde. Andererseits ist nun aber auch die Autorität über die *Nutzung* von Kryptographie dezentralisiert. Nicht mehr nur die

Bei genauerer Betrachtung fällt aber auf, dass auch hier die Sachlage hinsichtlich der Transparenz der Mächtigen weitaus komplexer ist. Könnte es sein, dass die Kryptographie ironischerweise *auch* die Transparenz der Mächtigen fördert und fordert – dass über die Jahrtausende Kryptographie das Mittel zum Machterhalt, zur Verschlüsselung, zur elitären Abschottung war, nun aber zur Transparenz zwingt? Im Folgenden wird argumentiert, dass die Kryptographie *unter bestimmten Umständen*[19] tatsächlich die Transparenz der Mächtigen fördert. Dazu ist das sogenannte *Whistleblowing* zu betrachten.

Im hier besprochenen Sinne meint *Whistleblowing* die unautorisierte Meldung von empfundenem Fehlverhalten mithilfe der Veröffentlichung oder Weiterleitung von unter Verschluss gehaltenen Informationen.[20] Diese Informationen müssen dabei nicht staatlicher Natur sein, sondern können auch von Unternehmen oder anderen Organisationen stammen. Historisch betrachtet fanden in den letzten Jahrzehnten einige der spektakulärsten Whistleblowing-Aktionen aller Zeiten statt – so etwa durch Chelsea Manning, die der Plattform *Wikileaks* Dokumente zum Irak-Krieg zuspielte, oder wenige Zeit später durch Edward Snowden, der das Wirken der NSA einer breiten Weltöffentlichkeit zugänglich machte.[21]

Als Motive nennen Whistleblower oftmals idealistische, altruistische oder ethische Gründe wie die Veröffentlichung von Unrechtmäßigkeiten, Misswirtschaft und Korruption.[22] In diesen Fällen wollen sich Whistleblower zur Wehr setzen, insofern sie davon ausgehen, die Veröffentli-

---

Mächtigen der Welt können Kryptographie nutzen, sondern jedes Individuum. Ursprüngliche Machtasymmetrien im Bereich der vertraulichen Kommunikation können mit einer solchen Kryptographie abgebaut werden.

19 Diese Einschränkung ist essentiell notwendig, wie noch deutlich werden wird. Manche Cypherpunks scheinen diesen Aspekt zu wenig bedacht zu haben.

20 Siehe zu Definitionen des Whistleblowings Jason Ross Arnold. *Whistleblowers, Leakers, and Their Networks: From Snowden to Samizdat*. Lanham u. a.: Rowman & Littlefield, 2020, S. 12–20, sowie Emanuela Ceva und Michele Bocchiola. *Is Whistleblowing a Duty?*. Cambridge und Medford: Polity Press, 2019, zu einer präziseren Definition und den damit zusammenhängenden Schwierigkeiten vor allem S. 17–45; allgemeiner zum Whistleblowing Greenberg, *This Machine Kills Secrets*.

21 Siehe zu Manning einführend Ceva und Bocchiola, *Is Whistleblowing a Duty?*, S. 6–7; ausführlicher auch Greenberg, *This Machine Kills Secrets*, S. 14–46. Zu Snowden siehe Snowden, *Permanent Record*, sowie Greenwald, *No Place to Hide*, und einführend Webb, *Coding Democracy*, S. 65–68.

22 Siehe zu Motiven auch Ceva und Bocchiola, *Is Whistleblowing a Duty?*, S. 32–35. Nach der englischen Bezeichnung wird der Begriff *Whistleblower* im Folgenden im geschlechtsneutralen Sinne verwendet.

chung der Informationen könne eine entsprechende Wirkung erzielen. So nennt etwa auch Edward Snowden in seiner Autobiographie die Bedeutung der Information für die Öffentlichkeit:

> It was only when I came to a fuller understanding of this surveillance and its harms that I became haunted by the awareness that we the public – the public of not just one country but of all the world – had never been granted a vote or even a chance to voice our opinion in this process.[23]

Tatsächlich hatten die im *Guardian* erschienenen Snowden-Leaks nationale und internationale Debatten zum Einfluss der Geheimdienste zur Folge. Neben der im Fokus stehenden NSA waren dies auch Geheimdienste der übrigen Länder der sogenannten *Five Eyes* (neben den USA Australien, Großbritannien, Kanada und Neuseeland).[24] Allerdings soll es hier nicht um eine Bewertung des Whistleblowings *an sich* gehen. Axiomatisch betrachtet geht dieses Kapitel von der Annahme aus, dass die prinzipielle *Möglichkeit* des Whistleblowings normativ-ethisch als positiv zu bewerten ist.[25] Ob einzelne Whistleblower wie Snowden oder Manning ethisch richtig handelten, ist nicht Teil der Diskussion.[26] Die Frage, die sich für eine Ethik der Kryptographie aber stellt, ist: Welche Bedeutung

23 Snowden, *Permanent Record*, S. 6. Zu den weiteren Motiven siehe auch Robert Manne. „The Snowden files". In: *The Monthly* (Sep. 2014). URL: https://www.themonthly.com.au/issue/2014/september/1409493600/robert-manne/snowden-files (besucht am 15.04.2024).

24 Siehe einführend zu den Five Eyes Anderson, *Security Engineering*, S. 19–30 sowie S. 922–925.

25 Siehe zur Bewertung Ceva und Bocchiola, *Is Whistleblowing a Duty?*. Beispielsweise schreibt auch Glenn Greenwald: „Promoting the human capacity to reason and make decisions: that is the purpose of whistleblowing, of activism, of political journalism." Greenwald, *No Place to Hide*, S. 253. In dieser Arbeit wird Whistlenblowing zudem als Möglichkeit des zivilen Ungehorsames betrachtet. Im Kontext von Edward Snowden weist William E. Scheuerman auf eine solche Verbindung hin. Siehe William E. Scheuerman. „Whistleblowing as civil disobedience: The case of Edward Snowden". In: *Philosophy & Social Criticism* 40.7 (2014), S. 609–628.

26 Beispielsweise wird Edward Snowden von dem Militärethiker George Lucas kritisiert. Dieser spricht von „grave moral errors" und schreibt: „Snowden's premeditated actions were those of a comparatively young and insufficiently oriented newcomer to the NSA. They were decidedly *not* the result of sober judgements, reluctantly reached by a seasoned, experienced, thoughtful, and reflective organizational veteran." Lucas, *Ethics and Cyber Warfare*, S. 49, kursiv im Original. Kritische Stimmen zu Snowden finden sich auch in Bauer, *Secret History*, S. 364–370. Zu einer weiteren Analyse siehe auch Hasian, Lawson und McFarlane, *The Rhetorical Invention of America's National*

hat die Kryptographie für das Whistleblowing? Einerseits könnte man zunächst annehmen, dass Whistleblowing schwieriger wird, wenn Daten verschlüsselt sind. Je weniger eine Person auf unverschlüsselte Daten Zugriff erhält, desto weniger unverschlüsselte Informationen kann sie auch veröffentlichen. Auf der anderen Seite scheinen die spektakulären und weitreichenden Whistleblowing-Aktionen der letzten Jahre dieser Ansicht zu widersprechen.

Ein empirischer Vergleich des Whistleblowings *vor* dem Paradigma der Modernen Kryptographie mit dem Whistleblowing *nach* dem Paradigmenwechsel ist kaum möglich. Eine quantifizierbare Bewertung ist schon allein deswegen problematisch, da inzwischen *massenhaft* Informationen in irgendeiner Form gespeichert und verarbeitet werden. Viel bedeutsamer als die *Quantität* der Daten und des Whistleblowings sind aber ohnehin dessen *Qualität* und die dahinter stehenden *Prozesse*. Diese unterscheiden sich heute markant von denen der vordigitalen Zeit. Der Journalist Andy Greenberg, ein Kenner der Whistleblowing-Szene, analysiert dazu in seinem Buch *This Machine Kills Secrets*:

> The insider's drive to expose institutional secrets – to conscientiously blow the whistle or vindictively dump a superior's dirty laundry – has always existed. But the technology that enables the spellers of secrets has been accelerating its evolution since the invention of computing. With the dawn of the Internet, the apparatus of disclosure entered a Cambrian explosion, replicating its effective features, excising its failed components, and honing its methods faster than ever before.[27]

Dies unterscheidet also das Whistleblowing *vor* der Existenz des Internets von den Möglichkeiten heute. Whistleblowing ohne Internet ist nicht nur teuer, sondern auch aufwendig und wesentlich leichter zu detektieren. Tausende Seiten an Dokumenten zu stehlen würde mehr auffallen, als einen kleinen USB-Stick herauszuschmuggeln. Was zuvor Monate dauern konnte, ist nun mit einem Klick möglich. Der Aufwand (und schließlich auch die Gefahr des Entdeckt-Werdens) scheint vor der Entwicklung des Internets ungemein höher gewesen zu sein. Um ein Beispiel zu nennen, auf das Andy Greenberg hinweist: Einer der bekanntesten Whistleblower des letzten Jahrhunderts – der US-Amerikaner Daniel Ellsberg – benötigte

Security State, S. 179–208. Für eine umfassende Einschätzung von Snowdens Wirken lohnt sich jedoch eine eigenständige Lektüre der Leaks und Veröffentlichungen.

27 Greenberg, *This Machine Kills Secrets*, S. 5.

fast ein Jahr, um die später als *Pentagon Papers* bezeichneten Dokumente zu kopieren.[28]

Trotzdem reicht diese Erklärung nicht aus, da die Frage bleibt: Warum kann die Kryptographie dies nicht verhindern, wenn sie inzwischen doch nicht mehr zu brechen sei? Wenn Geheimdokumente etwa mit AES verschlüsselt sind, wer könnte dann noch Whistleblower werden? Diese Fragen betreffen im Kern die Thematik von *Privacy for the weak, transparency for the powerful*. Doch auch hier gilt wieder ein entscheidendes Faktum, auf das in den letzten Kapiteln immer wieder hingewiesen worden ist: Kryptographie existiert nicht im Vakuum. Sie ist in der Anwendung immer eingebettet in soziale, gesellschaftliche, wirtschaftliche und technologische Kontexte.

Wie bereits in der Diskussion des *Going-Dark-Problems* analysiert worden ist, ist Kryptographie keine *hinreichende* Bedingung zur Vertraulichkeit. Sie ist technisch, organisatorisch und personell *immer* eingebunden durch *Umgebungsfaktoren*. Diese Umgebungsfaktoren bestimmen mit, ob Aufbewahrung und Kommunikation tatsächlich sicher und vertraulich sind. Beispielsweise ist es möglich, dass Geheimdokumente mit AES verschlüsselt sind. Diese Geheimdokumente sind daraufhin nicht ohne den dazugehörigen Schlüssel entschlüsselbar. Aber auch mit solchen Geheimdokumenten werden Organisationen und Personen arbeiten müssen. Ein gewisser Personenkreis und gewisse Teile einer Institution oder Organisation werden Zugriff auf diese Dokumente erhalten. Je größer dieser Personenkreis ist, desto größer ist auch die Wahrscheinlichkeit, dass sich eine Person dieses Kreises zum Whistleblowing entscheidet.

Dem liegt eine grundsätzliche Asymmetrie zugrunde, die das Verhältnis von Geheimhaltung und Veröffentlichung beschreibt: Es genügt bereits *eine einzige Person*, die sich zur Veröffentlichung durchringt. Anders gesagt müssen sich zur erfolgreichen Geheimhaltung der Dokumente *alle Personen* gegen ein Whistleblowing entscheiden. Die Kryptographie und damit die Möglichkeit vertraulicher und in gewissem Rahmen anonymer Kommunikation bietet hierfür die entscheidende Grundlage. Es scheint also so, als würde das Bedeutungsgewicht der Kryptographie aufseiten des Whistleblowings liegen: Kryptographie kann zwar dafür sorgen, dass Daten verschlüsselt und vertraulich sind, sie kann aber nicht garantieren, dass die Umgebungsfaktoren eine solche Verschlüsselung nicht

28 Siehe ebd., S. 13.

doch nutzlos machen, und darüber hinaus kann sie Personen beim Whistleblowing unterstützen, indem sie es ihnen ermöglicht, vertraulich und anonym zu kommunizieren.[29]

Hatten die Cypherpunks also womöglich doch recht, als sie einerseits Kryptographie fördern und andererseits die Geheimhaltung von Information reduzieren wollten? Ist die Macht der Mathematik geeignet, die Mächtigen zur Transparenz zu zwingen, die Schwachen aber zu beschützen? Sind Verschlüsselung und Geheimhaltung (engl. *secrecy*) für die Crypto-Anarchie nun nicht mehr dasselbe? Für May löst sich dieser scheinbare Widerspruch wie folgt auf:

> [C]rypto-anarchy doesn't mean a "no secrets" society; it means a society in which individuals must protect their own secrets and not count on governments or corporations to do it for them. It also means "public secrets," like troop movements and stealth production plans, or the tricks of implanting wafers, will not remain secret for long.[30]

Es ist also gerade jene Technologie, die die Geheimdienste zur Geheimhaltung nutzen wollten, die das Whistleblowing erst in dieser Form ermöglicht. Das bekannteste Beispiel für eine solche Verbindung von Kryptographie und Whistleblowing ist die Plattform *Wikileaks* des australischen Cypherpunks Julian Assange.[31] Die prinzipielle Möglichkeit der anonymen, nicht-identifizierbaren und vertraulichen Kommunikation von Whistleblowern, Journalistinnen und Journalisten sowie Plattformen wird dabei zu einer Voraussetzung für das Whistleblowing. Etwas ironisch verbindet daher die Moderne Kryptographie einerseits Privacy und andererseits Transparenz. Ohne eine freie und zugängliche Kryptographie wäre Whistleblowing nicht in dieser Form möglich, insofern es keine Möglichkeiten zur vertraulichen, anonymen und trotzdem digitalen Kommunikation

29 Zumindest können Whistleblower Zeit gewinnen; bis es dazu kommt, dass Identität und Person festgestellt werden können – das dürfte nach Veröffentlichung der Daten recht bald der Fall sein –, kann die Flucht geplant oder juristischer Rat eingeholt werden. Allerdings bleibt auch für den Whistleblower die Problematik bestehen, dass die Kryptographie keine *hinreichende* Bedingung zur vertraulichen und anonymen Kommunikation darstellt.

30 Zitiert in Greenberg, *This Machine Kills Secrets*, S. 90–91; genannt auch in Anderson, „Privacy for the weak, transparency for the powerful", S. 300.

31 Siehe zur umfassenden Einführung Greenberg, *This Machine Kills Secrets*; für eine kritische Analyse auch Arnold, *Whistleblowers, Leakers, and Their Networks: From Snowden to Samizdat*, S. 109–135.

gäbe. In den Worten von Andy Greenberg bedeutet das: „The craft of cryptographic leaking that Wikileaks brought to light seems like a paradox: A movement focused on divulging secrets depends on a technology invented to keep them."[32]

Wenn wir so auf das Cypherpunk-Ideal *Privacy for the weak, transparency for the powerful* zurückkommen, dann ist einerseits deutlich geworden, dass die Kryptographie tatsächlich Privacy für die Schwachen unterstützt. Mehrfach ist eruiert worden, dass sie dafür sogar eine *notwendige* Bedingung darstellt. Gleichzeitig zeigt der Exkurs über das Whistleblowing, dass Kryptographie ironischerweise auch die Transparenz der Mächtigen fordert. Sie ist in der Anwendung schließlich kein *hinreichendes* Mittel zur Vertraulichkeit von Information. In (über-)mächtigen und autoritären Organisationen und Strukturen kann Kryptographie nie alleiniges Mittel zur Intransparenz sein. Zwangsläufig haben Teile und Personen der Organisationen Kenntnis von klassifizierten Informationen. Ermöglicht bereits eine einzige Person, sei es aufgrund einer moralischen Gewissensentscheidung oder aus opportunistischen Erwägungen, die Deklassifikation in Zusammenarbeit mit Medien und Journalismus, kann die Kryptographie hierbei wieder als Schutz für diese eine Person dienen.

Und trotzdem hatten manche Crypto-Utopistinnen und -Utopisten nicht in allem recht. Das Problem ist in diesem Fall, dass es für sie auch hier wieder eine zu starke *Natürlichkeit* geben würde. Das Internet *musste* in Verbindung mit Kryptographie dazu führen, dass geheime Informationen publik werden – oder mit einem bekannten Spruch plakativ ausgedrückt: *Information wants to be free*.[33] Deskriptiv also, nicht normativ. Auch bei Wikileaks soll es eine Art *Natürlichkeit* gegeben haben. Greenberg etwa schreibt, Wikileaks sei der „*inevitable* outcome of the changing nature of information and advancements in cryptographic anonymity" gewesen.[34] *Unausweichlich*, *natürlich*, *alternativlos* – das also, was Lessig *is-ism* nennt.[35]

Kryptographie ist aber auch aus der Perspektive des Whistleblowers in soziale, technologische und oftmals auch wirtschaftliche Kontexte eingebettet. Whistleblowing kann nur dann erfolgreich sein, wenn auch die

32 Greenberg, *This Machine Kills Secrets*, S. 6.

33 Zitiert und besprochen beispielsweise in Borsook, *Cyberselfish*, S. 35, sowie in Goldsmith und Wu, *Who Controls the Internet?*, S. 51–52.

34 Greenberg, *This Machine Kills Secrets*, S. 7, kursiv im Original.

35 Siehe Lessig, *Code*, S. 31–37.

Medien, die Gesellschaft sowie die Journalistinnen und Journalisten bereit dafür sind. Dies gilt insbesondere dann, wenn auf langfristige Sicht Repressionen und Benachteiligungen zu erwarten sind. Edward Snowden wusste, dass er fliehen musste – trotz der Möglichkeit verschlüsselter Kommunikation. Julian Assange sah sich jahrelangen Prozessen um seine Auslieferung ausgesetzt – trotz der Möglichkeit verschlüsselter Kommunikation. Und Chelsea Manning saß mehrere Jahre in Haft für die Veröffentlichung von Missständen im Irak-Krieg – trotz der Möglichkeit verschlüsselter Kommunikation. Auch für Whistleblower ist Kryptographie kein hinreichendes Mittel.

Dieses Faktum scheinen manche Crypto-Anarchistinnen und -Anarchisten zu wenig bedacht zu haben. Kryptographie *allein* wird kein allgegenwärtiges Whistleblowing im Sinne des Aufdeckens von Missständen ermöglichen. Kryptographie wird es zwar fördern, benötigt aber stets auch Unterstützung von Einzelnen, der Politik und der Gesellschaft. In einer Gesellschaft, in der Whistleblowing als *generelle* Gefahr für die nationale Sicherheit betrachtet wird, oder in einer Autokratie, die mit harten Repressionen gegen Journalistinnen und Journalisten vorgeht, wird das Whistleblowing offensichtlich weiterhin unattraktiv sein – so idealistisch auch manche Personen beim Whistleblowing zu sein scheinen.

Kryptographie kann nur unterstützen, die Möglichkeiten für ein Whistleblowing zu erweitern und die Schäden für die Personen zu minimieren. Wenn wir axiomatisch davon ausgehen, dass die *Möglichkeit* des Whistleblowings *gut* ist, dann ist auch eine freie, zugängliche und sichere Kommunikation mithilfe kryptographischer Verfahren geboten. Gesellschaft und Politik sind dann aber gefordert, die Rahmenbedingungen für eine florierende Kryptographie bereitzustellen. Die Vorteile der Kryptographie werden nur *unter diesen bestimmten Umständen* zu erreichen sein. Wenn sich Staaten jedoch entscheiden, eine Ende-zu-Ende-Verschlüsselung zu verbieten, oder wenn Gesellschaften nach mehr Überwachung des Individuums trachten, dann wird dies auch unweigerliche Folgen für das Verhältnis von Whistleblowing und Kryptographie haben.

Für die Ausgangsidee des *Privacy for the weak, transparency for the powerful* bedeutet das letztlich, dass eine freie und zugängliche Kryptographie eine Umkehrung autoritärer Strukturen sowohl *unterstützt* als auch *voraussetzt*. Ob wir Kryptographie und deren Einsatz letztlich normativ positiv bewerten möchten, hängt davon ab, ob wir eine Prämisse von Privacy für den Einzelnen oder die Prämisse der Möglichkeit des Whist-

leblowings akzeptieren. Wenn wir bereits eine von beiden annehmen, dann wird auch die ubiquitäre Kryptographie zur notwendigen Bedingung. Einen anderen Mittelweg oder einen Kompromiss kann es mit der technologischen Realität der Kryptographie nicht geben.

7.2 Egalitäre Kryptographie

Moderne Kryptographie ist (1) Wissenschaft (2) mit dem Ziel der Sicherheit von Systemen und (3) nutzbar für gewöhnliche Menschen überall auf der Welt.[36] Teil I hat bereits das erste und das zweite Merkmal aus technologischer und mathematischer Sicht erläutert. Dieser Abschnitt wird nun das dritte Merkmal genauer untersuchen. Alle drei werden im Folgenden als notwendige Bedingungen einer *egalitären Kryptographie* definiert. Hinzu kommt aber eine weitere notwendige Bedingung, damit die egalitäre Kryptographie zur Realität werden kann: (4) Kryptographie muss auch *tatsächlich* von allen genutzt werden.

Auf andere Art formuliert beschreibt eine solche egalitäre Kryptographie einerseits die Art und Weise, wie sie entwickelt, implementiert und schließlich genutzt wird. Darüber hinaus verweist sie aber auch auf das, was Kryptographie *und deren Anwendung* für Demokratien, liberale Gesellschaften und soziale Partizipation bedeuten. In diesem Kontext kann eine Top-down- vs. Bottom-up-Kryptographie unterschieden werden. Eine Top-down-Kryptographie ist das, was unter anderem als Klassische Kryptographie verstanden wird: vorgegeben durch Geheimdienste, Militär, Diplomatie. Eine Bottom-up-Kryptographie hingegen ist konzeptuell vergleichbar mit der *Free-and-Open-Source-Software*-Bewegung (FOSS), bei der nicht primär ökonomische Interessen im Vordergrund stehen, sondern unter anderem die Partizipation an der Entwicklung und Community-getriebene Fortschritte.[37] Dass FOSS-Produkte ähnlich erfolgreich sein können wie proprietäre Software, zeigt etwa das von Linus Torvalds entwickelte Betriebssystem *Linux*.

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

37 Siehe zur Einführung in die FOSS-Kultur etwa Coleman, *Coding Freedom*. *Open Source* meint allerdings nicht das Gleiche wie *free software*. Dieser Aspekt wird in den Diskussionen nicht weiter behandelt. Siehe dazu Webb, *Coding Democracy*, S. 26–27, allgemein einführend auch S. 22–29.

Ein Beispiel für eine solche Bottom-up-Kryptographie ist Phil Zimmermanns *Pretty Good Privacy* (PGP).[38] Auch wenn PGP ursprünglich die Idee eines Einzelnen war, entwickelte sich rasch eine florierende Community, die sich den Prinzipien freier und zugänglicher Software verpflichtet fühlte. Die ethische Bedeutung eines solchen Wirkens kann kaum überbetont werden: Die Implementierung von Kryptographie war nicht mehr vorgegeben durch eine staatliche Institution oder ein Unternehmen, wie es lange Zeit zuvor noch der Fall gewesen war. Nicht die NSA, nicht IBM, nicht eine andere zentralistische Organisation war es, die letztlich zum ersten Mal der *gesamten* Welt eine praktisch implementierte Kryptographie zugänglich machte, sondern eine Gemeinschaft aus idealistischen Nerds, die mit technologischer Entwicklung ethisch handeln wollten. Ein solcher *Open Code* wird, wie es Lessig nennt, dann auch zu einem „constraint on state power“[39].

PGP war einerseits nicht lokal durch Exportbeschränkungen oder Patentstreitigkeiten zu begrenzen. Da die grundsätzliche Mathematik hinter dem DH-Schlüsselaustausch und RSA bekannt war, war auch die Implementierung möglich. Um Exportbeschränkungen zu umgehen, genügte es, den Code auf Papier zu drucken und daraufhin zu versenden, womit er am Zielort wieder eingescannt werden konnte.[40] Andererseits konnte verschlüsselte Kommunikation nun von mehr Menschen genutzt werden, als dies jemals zuvor der Fall gewesen war. Diese Bottom-up-Kryptographie führt dazu, dass Kryptographie ubiquitär und global wird. Das dritte Merkmal der Modernen Kryptographie, wonach Kryptographie für gewöhnliche Menschen überall auf der Welt nutzbar wird, wird damit erfüllt.

Um die Normativität der freien, unbeschränkten und egalitären Kryptographie aber noch präziser zu untersuchen, betrachten wir diesen *globalen Anspruch*. Würden wir die Kryptographie nämlich nur lokal oder aus der Perspektive liberal-demokratischer Staaten diskutieren, dann würden wir deren Potential nicht in Gänze erfassen. Auch in freiheitlichen

38 Siehe ausführlicher Abschnitt 3.1 sowie Levy, *Crypto*, S. 204.

39 Lessig, *Code*, S. 139. Letztlich bedeutet aber ein offener Quellcode und eine Open-Source-Community nicht nur eine Einschränkung für die Staatsmacht, sondern auch für das Patent-fokussierte Unternehmertum, das Software möglichst verschlossen und lizenzierbar halten möchte. Eine gewisse Ironie von Transparenz, Verschlüsselung und Geheimhaltung, die bereits zuvor analysiert worden ist, ist daher auch hier nicht zu übersehen.

40 Siehe dazu Kapitel 3 und Kapitel 4.

Staaten könnte man geneigt sein anzunehmen, dass eine Beschränkung oder Regulierung von Kryptographie zur verschlüsselten Kommunikation sinnvoll ist. Womöglich gäbe es genügend demokratische Kontrolle und wohl auch Beschränkungen des staatlichen und unternehmerischen Einflusses. Doch gilt es auch zu erkennen, dass unsere *lokal* entwickelte Kryptographie – respektive unsere *lokal* regulierte Kryptographie – *globale* Auswirkungen hat. Kryptographie fördert die Teilhabe am Informationsaustausch, am Verhindern von Zensur, am Widerstand von Unterdrückung. Mit der Kryptographie, die in liberalen Gesellschaften entwickelt wird, werden Werte implementiert, die global exportiert werden können.[41]

Dies bedeutet dann aber auch: Wenn Gesellschaften diese Werte, Menschenrechte und Prinzipien global exportiert und realisiert sehen wollen, dann muss eine Beschränkung, Reduktion oder Regulierung der Forschung, Anwendung und Nutzung von Kryptographie abgelehnt werden. Umgekehrt gilt: Wenn dies in als liberal angesehenen Gesellschaften *nicht* geschieht, dann werden die liberalen Werte wie Freiheit der Meinungsäußerung, des Privatlebens oder der Vertraulichkeit der Kommunikation auch *nicht* durch eine Kryptographie im globalen Kontext gefördert werden.

Deskriptiv betrachtet ist eine solche Kryptographie, die als *egalitäre Kryptographie* bezeichnet werden soll, bislang nicht vollständig umgesetzt, sofern das oben genannte vierte Kriterium einer *tatsächlich* von allen genutzten Kryptographie hinzukommt. Eine quelloffene Kryptographie schafft zwar global eine freie und zugängliche *Möglichkeit* der verschlüsselten Kommunikation. Doch genügt das nicht. Kryptographie wird erst dann zur egalitären Kryptographie, wenn sie auch genutzt wird.

Es ist jedoch zu bezweifeln, dass dieses Kriterium der *Angewandtheit* bereits immer und überall erfüllt ist. Weder medial noch in den nicht-

41 Ein Beispiel ist hier Sina Rabbani. Der Iraner entwickelt und betreibt Verschlüsselungstechnologien in den USA, um Protestbewegungen im Iran zu unterstützen. Berichtet wurde davon vor allem in Avi Bolotinsky, Anita Ritscher und Philip Cheung. „Dieser Iraner kämpft im Internet für Freiheit". In: *Neue Zürcher Zeitung* (3. Juni 2023). URL: https://www.nzz.ch/technologie/sina-rabbani-ein-iranischer-freiheitskaempfer-im-internet-ld.1733694 (besucht am 15.04.2024). Siehe zu einer internationalen Perspektive auf die Kryptographie auch Kevin Macnish. „An End to Encryption? Surveillance and Proportionality in the Crypto-Wars". In: *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*. Hrsg. von Adam Henschke u. a. Cham: Springer, 2021, S. 155–173.

technischen Wissenschaften werden Kryptographie und deren Bedeutung umfassend diskutiert. Auch in der Gesellschaft scheint die Motivation, sich mit Verschlüsselung auseinanderzusetzen, gering zu sein. Folglich genügt es nicht, wenn nur eine Gruppe aus Entwicklerinnen und Entwicklern an Implementierungen arbeitet – sofern der Drang des gewöhnlichen Individuums überhaupt nicht vorhanden ist, Kryptographie zu nutzen. Man könnte plakativ sagen: *Imagine there is cryptography – and nobody uses it*. Kryptographie wird aber erst dann zur egalitären Kryptographie, wenn sie *faktisch* genutzt wird.

Zu unterscheiden ist daher zwischen der Kryptographie als Mathematik, die weder normativ noch regulierbar ist, und der *Anwendung* der Kryptographie. Die Komplexität der Verschlüsselung, die vielen verschiedenen Facetten von Informationssicherheit und schließlich die mathematische Spezialisierung Moderner Kryptographie lassen nämlich dem gewöhnlichen, technologisch unbedarften Individuum wenig Raum zur *aktiven* Teilhabe an der Möglichkeit verschlüsselter Kommunikation. Das gewöhnliche Individuum muss sich angesichts dessen darauf verlassen, dass wiederum *andere* dafür sorgen, dass eine Verschlüsselung tatsächlich sicher und vertraulich ist – und nicht etwa doch eine Backdoor implementiert wurde. Das Ausmaß des erforderlichen Vertrauens wird zwar dadurch verringert, dass es auf zahlreiche Entwicklerinnen und Entwickler eines quelloffenen Codes verteilt wird. Ganz ohne Vertrauen geht es allerdings auch in der Kryptographie nicht.

Es scheint, als hätten Crypto-Utopistinnen und -Utopisten diese Unterscheidung von Mathematik einerseits und deren *tatsächlicher* Anwendung andererseits zu wenig bedacht. Beide Aspekte, sowohl das mangelnde Interesse gewöhnlicher Individuen als auch die Notwendigkeit des Vertrauens, sind jedoch aus normativer Perspektive relevant. Die Existenz einer mathematisch rigorosen Kryptographie *alleine* genügt eben nicht, um deren Vorteile in der Praxis auch einzusetzen. Wenn günstige sozial-gesellschaftliche Umstände dazu nicht vorhanden sind, wenn zudem Unwissenheit (engl. *illiteracy*) hinsichtlich der Bedeutung der Kryptographie besteht, dann wird auch der Erfolg von Software wie PGP beschränkt bleiben.

In der Crypto-Anarchie ist man vielleicht immer davon ausgegangen, dass Kryptographie nie *vollständig* unterdrückt werden *kann*. Damit hatten die Vertreterinnen und Vertreter dieser Strömung durchaus recht. Doch liegt hier ethisch betrachtet die Gefahr, dass es zu einer *unvollständigen* Regulierung kommt. Bei einer Unterdrückung und Regulierung von

Kryptographie ging es ja nie darum, dass sie *für alle und jeden* umsetzbar sein wird. Offensichtlich kann Mathematik nicht reguliert werden, und auch der Austausch von Software im Internet lässt sich nicht überall unterbinden. Das Ziel einer Regulierung von Kryptographie besteht denn auch vielmehr darin, *den meisten Menschen* diese Möglichkeit zu verwehren.[42] Julian Assange – der an dieser Stelle eine andere Philosophie verfolgt wie etwa Tim May[43] – bringt einen solchen Gedanken auf den Punkt, wenn er sagt:

> [P]erhaps there will just be the last free living people, those who understand how to use this cryptography to defend against this complete, total surveillance, and some people who are completely off-grid, neo-Luddites that have gone into the cave, or traditional tribes-people who have none of the efficiencies of a modern economy and so their ability to act is very small.[44]

Wenn Kryptographie zur vertraulichen und zudem auch anonymen Kommunikation reguliert oder gar unterdrückt wird, dann bedeutet dies in der Folge eine Verstärkung der *Ungleichheit*. Es gibt in einer solchen Welt eine kleine, technologisch versierte Gruppe, die weiter per Ende-zu-Ende-Verschlüsselung kommunizieren kann, zum Beispiel per Open-Source-Software.[45] Daneben steht die andere Gruppe, technologisch weniger bewandert, die dies nicht mehr tun kann und so auch nicht tun wird. Diese Ungleichheit besteht schon jetzt, denken wir an die Entwicklerinnen und Entwicklern auf der einen und die *gewöhnlichen Individuen* auf der anderen Seite.[46] Die Macht, die Kryptographinnen und Kryptographen angesichts dessen haben können, würde im Falle einer Regulierung oder Beschränkung nur noch größer im Verhältnis zu gewöhnlichen Menschen. Eine Regulierung der Nutzung von Kryptographie führt so nur zu

42 In den Worten von Lessig: „And even if not impossible, sufficiently difficult for the vast majority of us." Lessig, *Code*, S. 54.

43 Siehe Webb, *Coding Democracy*, S. 52. Für May ging es nicht um die Gesellschaft als Ganzes, sondern um das eine Prozent der Bevölkerung, für das die Kryptographie von Vorteil sein wird. Siehe Bartlett, *The People Vs Tech*, S. 189.

44 Assange u. a., *Cypherpunks*, S. 62–63.

45 Siehe Moore und Rid, „Cryptopolitik and the darknet", S. 31.

46 Ähnlich schreibt Maureen Webb: „Code, more than law, will soon determine what kind of societies we live in and whether they end up resembling democracies at all. Yet code is incomprehensible to most people, myself included. Computer users, for the most part, are at the mercy of the code makers." Webb, *Coding Democracy*, S. 3.

noch mehr Ungleichheit, die im Sinne einer chancengerechten, liberalen und egalitären Gesellschaft inkompatibel mit Grund- und Menschenrechten ist. Die Verminderung einer solchen Ungleichheit kann nur gelingen, wenn auch gewöhnliche Individuen Zugriff auf sichere Verschlüsselungsverfahren erhalten und diese *tatsächlich auch nutzen*.[47]

Diese Ungleichheit im Hinblick auf Kryptographinnen und Kryptographen, auf die Entwicklerinnen und Entwickler ist offensichtlich. *Cryptography is law* – und wenn wir die Anwendung der Kryptographie reduzieren, werden just jene Gruppen noch stärker zu *lawmakers* ohne demokratische Legitimation.[48] Gleichzeitig ist auch eine andere Gruppe zu berücksichtigen. So haben *Kriminelle* ein inhärentes Interesse an verschlüsselter Kommunikation. Dieses Interesse wird auch eine egalitäre Kryptographie nicht reduzieren. Allerdings, und dies ist der entscheidende Punkt, wird auch eine reduzierte und regulierte Kryptographie das nicht schaffen. Wenn Kryptographie und vor allem deren Anwendung komplex, unsicher und sinnlos scheint, dann werden interessierte Kriminelle alles daran setzen, Lösungen und Alternativen zu entwickeln. Es ist unwahrscheinlich, dass eine Regulierung – sei sie direkt oder per Intermediäre – dies erfolgversprechend verhindern könnte. Paradoxerweise könnte es durch eine Reduktion der Verschlüsselung sogar zu *mehr* Verschlüsselung kommen, die aber, wie Moore und Rid erkennen, den Kriminellen helfen dürfte:

> Any attempt to systematically undermine end-to-end encryption – through legislation requiring service providers to retain the option of removing encryption for any given user – will likely strengthen more secure implementations by creating more demand for them, and thus help criminals and militants. We believe it should be a political no-go area for democratically elected governments to pursue such a path.[49]

Solch eine egalitäre Kryptographie ist aber nicht nur konsequentialistisch geboten, sondern hängt eng mit einer anthropologischen Perspektive auf die Kryptographie zusammen. Die Idee von Privacy, von abgeschotteter Kommunikation ist letztlich zurückzuführen auf die grundsätzliche

47 Siehe weiterführend zur Verantwortung von Kryptographinnen und Kryptographen Rogaway, *The Moral Character of Cryptographic Work*.

48 In Anlehnung an Lessig, *Code*, S. 5.

49 Moore und Rid, „Cryptopolitik and the darknet", S. 31–32.

und immer schon vorhandene Möglichkeit, dass Individuen sich von der Gesellschaft in einen privaten und geschützten Raum zurückziehen können. In diesem Raum können sie kommunizieren, ohne ein Abhören der Kommunikation befürchten zu müssen. Die *latent ambiguity* der Kryptographie lässt sich also auflösen, indem verschlüsselte Kommunikation als anthropologische Notwendigkeit betrachtet wird. Ähnlich schreiben auch Diffie und Landau:

> [I]f we deny the fact that telecommunication, whatever its new properties, is rooted in face-to-face conversation and shares much of its social function, we will doom ourselves to a world in which truly private conversation is a rarity – a perquisite belonging exclusively to the well-traveled rich.[50]

Sie nennen hier eine weitere Gruppe, die für die Ungleichheit der vertraulichen Kommunikation relevant ist: die Reichen und Vermögenden. Diese müssen zwar nicht kryptographisch versiert sein, doch werden sie über das Kapital verfügen, eine solche kryptographische Unterstützung zu erwerben. Auch hier wird keine Regulierung dazu führen, dass dies für die Reichen und Mächtigen nicht mehr gilt. Gleiches ist auch bei staatlichen Akteuren anzunehmen, die die Möglichkeit der verschlüsselten Kommunikation für sich selbst trotz einer gesellschaftlichen Regulierung nicht aufgeben werden. Als Begründungen könnten Themen angeführt werden wie die nationale Sicherheit oder Geheimdienstinteressen.[51] Nur eine egalitäre Kryptographie kann dafür sorgen, dass eine gesellschaftliche Asymmetrie der vertraulichen Kommunikation reduziert wird.[52]

Die Gefahr der Ungleichheit der Kryptographie betrifft also nicht nur die Ungleichheit zwischen gewöhnlichen Menschen einerseits und Kryptographinnen und Kryptographen andererseits, sondern geht weit darüber hinaus. Von gewöhnlichen Individuen kann weder erwartet werden, dass sie sich mit Verschlüsselungstechnologien auseinandersetzen, noch können wir davon ausgehen, dass sie dafür entsprechendes Kapital

50 Diffie und Landau, *Privacy on the Line*, S. 10.

51 Solch ein Argument ist keine reine Spekulation. Als Beispiel kann hier das Client-Side-Scanning dienen, für das staatliche Ausnahmen erwogen wurden. Siehe Abschnitt 8.1.

52 Der deutsche Mathematiker Albrecht Beutelspacher formuliert es normativ: „Kryptographische Algorithmen sind heute kein Privileg der Geheimdienste, sondern ein Allgemeingut, das jedem Bürger zugänglich sein muss." Beutelspacher, *Geheimsprachen und Kryptographie*, S. 112.

aufwenden. Egalitäre Kryptographie bedeutet hingegen, dass Kryptographie frei, zugänglich und nutzbar ist – und *tatsächlich* auch genutzt wird. Wenn eine Gesellschaft egalitär sein möchte, dann benötigt sie auch eine egalitäre Kryptographie. Die *tatsächliche Nutzung* von Verschlüsselung wird zur Metrik und zum Ziel einer Ethik der Kryptographie.

Oben sind bereits Zweifel daran angedeutet worden, dass eine egalitäre Kryptographie schon vollständig realisiert ist. Bislang haben wir uns insbesondere mit Kryptographie zur vertraulichen Kommunikation auseinandergesetzt. Kapitel 6 hat jedoch auch diskutiert, welche Rolle Metadaten für die Strafverfolgungsbehörden und Unternehmen spielen können. Auch wenn eine Ende-zu-Ende-Verschlüsselung des Inhalts erfolgt, schützt dies nicht per se davor, dass Metadaten gesammelt, aggregiert und analysiert werden. Für eine egalitäre Kryptographie sind Metadaten jedoch ebenso relevant, denn Technologien und Methoden, die *auch* eine Verschleierung von Metadaten erlauben, sind bei Weitem weniger ubiquitär als eine bloße Ende-zu-Ende-Verschlüsselung. In den Worten von Diffie und Landau bedeutet das:

> [I]t is very difficult for any individual or group within a society to protect its communications comprehensively. It can make use of end-to-end encryption but this will leave the pattern of communications visible. Any greater degree of protection, such as anonymity services, requires the society's cooperation or at least tolerance.[53]

Was bedeutet aber gesellschaftliche Kooperation oder zumindest deren Toleranz im Kontext einer egalitären Kryptographie? Welche Folgen hat dies für die oben beschriebene Ungleichheit? Zunächst bedeutet es, dass eine Ethik der Kryptographie sich nicht allein auf die Technologie selbst verlassen kann. Auch wenn die kryptographischen Methoden zur Verschleierung von Metadaten existieren, kann es sein, dass sie nicht genutzt werden – oder ihre Nutzung sogar absichtlich durch Unternehmen oder Institutionen erschwert wird. Das Paradigma der Modernen Kryptographie führt eben nicht *zwangsläufig* zur Anwendung einer personellen, vertraulichen und vor allem anonymen Kommunikation. Die Grundlagen Moderner Kryptographie können nicht unterdrückt werden, insofern sie Mathematik sind. Die Realisierung in der Anwendung *für jeden* ist jedoch

53 Diffie und Landau, *Privacy on the Line*, S. 112.

immer abhängig von der gesellschaftlichen Förderung und ethischen Akzeptanz.

Konkreter bedeutet gesellschaftliche Toleranz aber auch, dass es für Politik, Unternehmen und Gesellschaft nicht genügt zu sagen: *Keine Beschränkung von Kryptographie ist bereits gut genug.* Von zivilgesellschaftlichen Institutionen, staatlichen Parteien und wirtschaftlichen Unternehmen ist zur Realisierung einer egalitären Kryptographie mehr gefordert. Zunächst ist politisch ein egalitärer Bottom-up-Ansatz von Kryptographie *aktiv* zu fördern, der einen größeren, inklusiven Kreis zur Entwicklung und Nutzung von Kryptographie umschließt. Eine solche Bottom-up-Kryptographie ist eine entscheidende, praktikable und zudem kostengünstige Möglichkeit, eine egalitäre Kryptographie zu realisieren. In einem derartigen Prozess sollten auch Fragen nach der Nutzbarkeit der Kryptographie inkludiert werden, die es technologisch wenig bewanderten und marginalisierten Personengruppen ermöglicht, Verschlüsselungstechnologien intuitiv und niederschwellig zu nutzen.[54] Die immer wichtiger werdende Disziplin des *User Experience Design* ist hier im Besonderen gefordert.

Gleichzeitig setzt eine freie und zugängliche Kryptographie, die auch *faktisch* genutzt wird, ein ausreichendes Maß an Bildung (engl. *literacy*) voraus.[55] Diese Bildung muss die Bedeutung von Kryptographie für die Beseitigung oder Zurückdrängung möglicher Ungleichheiten bewusst machen und die positiven Aspekte, die an vielen Stellen in Bezug auf Privacy, Meinungsfreiheit und Anthropologie bereits diskutiert worden sind, herausstellen. Gleichzeitig sollte sie eine differenzierte Perspektive auf Gegenargumente wie das *Going-Dark-Problem* aufweisen, um allzu einfache Antworten gegen die Anwendung von Kryptographie entkräften zu können.

Diese Bildung sollte einerseits im Rahmen der Schul- oder Universitätslaufbahn erfolgen. Andererseits ist es aber ebenso wichtig, ein mediales und journalistisches Engagement zu fördern und zu fordern, um

54 So argumentiert etwa auch Glenn Greenwald dafür, dass die Tech-Community eine effektivere und nutzbarere Kryptographie entwickeln sollte. Siehe Greenwald, *No Place to Hide*, S. 252.

55 Schulz und van Hoboken erkennen hier auch: „There is an important role for education and training, and the more general goal that people should have a realistic idea of the risks that they face without being burdened with impossible requirements to protect oneself against unauthorized access to their content and communications." Schulz und Hoboken, *Human rights and encryption*, S. 63.

die Entwicklungen in der Kryptographie und die Möglichkeiten der Verschlüsselung auch denjenigen näherzubringen, die bislang keine aktiven Berührungspunkte damit hatten.[56] Zu einem solchen Schluss kommen auch Schulz und van Hoboken in ihrer überzeugenden Studie zu Menschenrechten und Kryptographie:

> Privacy protection should not just rest on the users making use of cryptographic technologies. Communicating the risks and spreading knowledge on the technologies should be a part of a national policy, with sufficient sensitivity of raising awareness among all users including various groups with different vulnerabilities such as journalists, women and girls, minorities, etc. States should be encouraged to make encryption literacy part of their communication as well as media and information literacy programs. Even though these measures might be limited in their effect, they remain an important element of any policy that puts the informed user in the centre.[57]

Egalitäre Kryptographie stellt die Nutzerin und den Nutzer in die Mitte des Geschehens. Egalitäre Kryptographie ist nicht bloß Mathematik oder Informationssicherheit. Egalitäre Kryptographie ist Moderne Kryptographie, die frei und zugänglich ist, vor allem aber auch *faktisch* und *von allen* genutzt wird. Bevor wir nicht an diesem Punkt sind, ist zu ihrer Realisierung politisches, wirtschaftliches und wissenschaftliches Engagement gefordert.

7.3 Identifikation mithilfe von Kryptographie

Die bisherigen Ausführungen haben sich vorwiegend mit der Kryptographie zur *Vertraulichkeit* beschäftigt. In diesem Kontext ist argumentiert worden, dass eine freie, zugängliche und tatsächlich genutzte Kryptographie ethisch geboten ist. Nun ist aber ein weiterer, konzeptuell neuer Bereich zu betrachten: die *Authentifizierung*. Zur Authentifizierung werden, wie bereits in Abschnitt 2.4 genannt, kryptographische Verfahren verwendet. Insbesondere sind dies *digitale Signaturen*, die auf dem Konzept der asymmetrischen Kryptographie aufbauen: Eine Nachricht wird mit dem eigenen, privaten Schlüssel signiert, und die Signatur wird zu-

56 Beispiele hierfür wären in den USA die *Electronic Frontier Foundation*, im deutschsprachigen Raum etwa die Plattform *netzpolitik.org*.

57 Schulz und Hoboken, *Human rights and encryption*, S. 63.

sätzlich zur Nachricht übertragen.[58] Die andere Partei kann, wenn sie die Authentizität einer Nachricht kontrollieren möchte, die Signatur mit dem dazugehörigen, öffentlichen Schlüssel überprüfen.[59]

Eng damit verbunden sind die Schutzziele der *Nicht-Abstreitbarkeit* und *Zurechenbarkeit*. In Kombination mit *Authentizität* soll also einem bestimmten Kommunikationspartner eine Nachricht zugeordnet werden können, diese Zuordnung soll überprüfbar sein und diese Zuordnung soll nicht im Nachhinein abstreitbar sein. Zu Recht gelten diese Aspekte als Schutzziele einer umfassenden Informationssicherheit. Hinzu kommen zudem juristische Fragen, die in digitalisierten Kommunikationsnetzen rechtliche Sicherheit erfordern. Zugleich ist auch die Authentifizierung Teil einer umfassenden Ethik der Kryptographie, da sie ein Hilfsmittel zur *Identifizierung* sein kann.[60] Und mit Identifizierbarkeit kehrt sich das bisherige Verhältnis von Kryptographie, Staat und Überwachung um. In den Worten des Kryptographen Ross Anderson: „Most crypto applications are about authentication rather than confidentiality, to help the police rather than hindering it."[61]

Für die Überwachung eröffnet sich qualitativ eine neue Dimension, sobald *auch* eine personenbezogene Identifikation möglich ist. Um dazu einige Beispiele zu nennen: Wenn die Fahrscheinkontrolle im öffentlichen Nahverkehr auch einen Ausweis verlangt, dann kann die Kontrolle (und alle damit verbundenen Systeme) nachvollziehen, dass *diese Person* an einem bestimmten Datum eine bestimmte Strecke gefahren ist. Wenn bei einer Krankenversicherung Identifikationsmerkmale erfragt werden, dann erlaubt dies die Verbindung einer *bestimmten Identität* zu einem gesundheitlichen Zustand. Wenn der Bibliotheksbestand so weit überwacht wird, dass auch erfasst wird, *wer* bestimmte Bücher liest, ist ein Profiling etwa

58 In der Praxis wird meist nicht die gesamte Nachricht signiert, sondern lediglich der Hashwert der Nachricht. Einerseits ist dies performanter, andererseits inkludiert dieser Prozess dann auch das Schutzziel der Integrität. Da moderne Hashalgorithmen wie SHA-3 als sicher gelten, ist dieser Prozess zu bevorzugen.

59 Whitfield Diffie und Susan Landau gehen sogar so weit zu sagen, dass die Schutzziele Authentizität und Integrität „arguably more important than privacy" seien. Diffie und Landau, *Privacy on the Line*, S. 12.

60 Bereits Lessig hat sich mit dieser Thematik auseinandergesetzt. Siehe Lessig, *Code*, S. 45–54, sowie Lawrence Lessig. „The Architecture of Privacy: Remaking Privacy in Cyberspace". In: *Vanderbilt Journal of Entertainment & Technology Law* 1.1 (1999), S. 56–65.

61 Anderson, *Security Engineering*, S. 928.

hinsichtlich politischer Interessen möglich.[62] Damit handelt es sich um einen konzeptuell neuen Bereich, der über eine reine Vertraulichkeit im Sinne der Schutzziele der Informationssicherheit hinausgeht.[63] Vielleicht ist eine Ausweiskontrolle im öffentlichen Verkehr unauffällig. Vielleicht ist bei einer Krankenversicherung eine digitale Abfrage der Identität kryptographisch sicher. Und vielleicht ist die Datenbank des Bibliotheksbestandes mit AES verschlüsselt. In allen diesen Fällen ist zwar Vertraulichkeit gegenüber Drittparteien gewahrt. Die *Identifizierung* bleibt jedoch zentraler Bestandteil der Kommunikation.

Auch Lessig hat sich in seinem bereits vielfach diskutierten Werk mit Identifizierungstechnologien beschäftigt.[64] Er zeigt hier, ganz im Sinne des *Code is Law*, zwei historische Modelle des Cyberspace, die eine Identifizierung im frühen Internet betrafen: einerseits an der University of Chicago, andererseits in Harvard.[65] In Chicago war ein Zugriff auf das Internet unkompliziert und unüberwacht möglich – „complete, anonymous, and free"[66]. Die Entscheidung, eine solche Architektur zu implementieren, entsprang weder der Natur noch sonstigen unüberwindbaren Voraussetzungen, sondern es war schlicht eine Entscheidung des Administrators. Für die Kryptographie ist in einem solchen Modell zwar technische Authentifizierbarkeit von Nachrichten weiterhin möglich, allerdings lässt sich keine Verbindung zwischen der realen Persönlichkeit und der Identität im Internet ziehen. Eine Nachverfolgbarkeit von Aktionen ist so nur schwer möglich.[67] In Harvard hingegen war der Zugang zum Internet

62 Letzteres ist nicht bloß hypothetische Spekulation oder Übertreibung, wie ein historisches Beispiel zeigt: Das *Library Awareness Program* des FBI zielte zwischen 1973 und 1988 darauf ab, Anfragen ausländischer Personen zu überprüfen. Zahlreiche Bibliothekare verweigerten jedoch die Auskunft. Siehe Diffie und Landau, *Privacy on the Line*, S. 165–166.

63 Siehe zur Identifikation einführend auch Solove, „A Taxonomy of Privacy", S. 511–516.

64 Siehe Lessig, *Code*, S. 45–54. Lessig weist auf die Unterscheidung von *confidentiality* vs. *identifictaion* hin. Siehe ebd., S. 53. Für ihn bedeutet das: „[Identity Technology] demonstrates the sense in which cryptography is Janus-faced"; ebd., S. 53. Seiner Ansicht nach wird das Internet zunehmend regulierbarer durch digitale Identifizierungstechnologien. Siehe ebd., S. x; weiterführend auch Lessig, „The Architecture of Privacy", vor allem S. 63.

65 Siehe Lessig, *Code*, S. 33–37. Hintergrund hierbei ist, dass das frühe Internet im universitären Bereich angesiedelt war und der Umgang mit ihm in der Administration unterschiedlich gehandhabt wurde.

66 Ebd., S. 33.

67 Siehe ebd., S. 34.

weitaus restriktiver gehandhabt: Eine Registrierung war erforderlich, und der Internetverkehr wurde überwacht – „licensed, approved, verified“[68], ganz im Kontrast zum Chicago-Modell.

Damit gab es in Chicago und in Harvard zwei Modelle, wie sie unterschiedlicher kaum sein können. Sie verdeutlichen, dass bereits in den frühen Jahren des Internets die Internet Policy eben nicht bloß eine reine Natürlichkeit war, sondern immer auch auf eine gezielte *Entscheidung* zurückging. Lessig bezeichnet das als „difference by design“[69]. In beiden Fällen wurden denn auch unterschiedliche Werte und Rechte implementiert: Im einen Fall war Nachverfolgbarkeit einfach möglich, im anderen deutlich schwieriger.[70] Bezogen auf den Aspekt der Kryptographie schreibt Lessig:

> In the Internet's first life, encryption technology was on the side of privacy. Its most common use was to keep information secret. But in the Internet's next life, encryption technology's most important role will be in making the Net more regulable. As an Identity Layer gets built into the Net, the easy ability to demand some form of identity as a condition to accessing the resources of the Net increases. As that ability increases, its prevalence will increase as well.[71]

Heute sind solche Identifikationsmaßnahmen vor allem durch *Know-Your-Customer*-Verfahren (KYC) bekannt, die unter anderem zur Bekämpfung von Geldwäsche im Bereich der Finanzinstitutionen und -dienstleistungen üblich sind. Aber auch in anderen Bereichen fassen zunehmend KYC-Verfahren Fuß, bei denen etwa eine Legitimation per amtlichem Ausweis erforderlich ist, zum Beispiel bei der Registrierung von SIM-Karten.[72] Auch Kryptowährungen wie Bitcoin, die einst in der öffentlichen Wahrnehmung fälschlicherweise als *irgendwie anonym* galten, erlauben durch KYC-Verfahren zunehmend Identifizierbarkeit.[73]

---

68 Ebd., S. 34.

69 Ebd., S. 34.

70 Siehe ebd., S. 34–36.

71 Ebd., S. 54. Lessig schreibt in einem anderen Artikel auch: „[E]ncryption may well reduce the searchable, by protecting what I hide; but by reducing the cost of authentication, it might well increase the monitored, and hence increase the searchable again. The technology, like much in this field, is Janus-faced-freedom-enhancing from one perspective, control-enhancing from another.“ Lessig, „The Architecture of Privacy“, S. 63.

72 Siehe etwa Kaye, *A/HRC/29/32*, para. 51.

73 Siehe weiterführend zur Anonymität von Kryptowährungen auch Abschnitt 3.3.

Für eine Authentifizierung ist zudem bedeutsam, dass die Identifizierung *transitiv* wirken kann. Um zur Verdeutlichung dieser Eigenschaft ein Beispiel zu nennen: Muss eine Person aufgrund gesetzlicher Vorgaben bei der Registrierung einer SIM-Karte einen Ausweis vorzeigen, wird dieser anschließend auf Echtheit überprüft. Danach registriert die betreffende Person sich auf bekannten Messengerdiensten, die eine Verknüpfung mit einer Telefonnummer erfordern. Erst jetzt kann die Person per Ende-zu-Ende-Verschlüsselung mit anderen Parteien kommunizieren, die den gleichen Prozess durchlaufen haben. Eine Identifizierbarkeit ist transitiv über die Registrierung der Telefonnummer per Identitätsnachweis gegeben. Nachdem hier mehrere Entitäten und Parteien involviert sind, ist der Aufwand für eine solche Identifizierung zwar nicht zu vernachlässigen. Die Kosten für einen solchen Datenaustausch sinken jedoch zunehmend, weshalb davon auszugehen ist, dass über die Zeit mehr solcher Identifikationsmöglichkeiten genutzt werden können.[74]

Um dieses Beispiel einordnen zu können, sind die regulatorischen Möglichkeiten von Identifizierungsmaßnahmen zu systematisieren. Ein Identifikationszwang, etwa ein digitaler Ausweiszwang zum generellen Internetzugang oder die Digitalisierung biometrischer Daten, kann zunächst *direkt* erfolgen. Eine solche Verpflichtung könnte wie folgt lauten: *Der Gesetzgeber verpflichtet Bürgerinnen und Bürger, sich ausschließlich mit ihrer digitalen ID in die sozialen Netzwerke einzuloggen.* Eine gesellschaftliche Ablehnung dieser Maßnahmen wäre wahrscheinlicher als bei einem *indirekten* Zwang über Intermediäre. Bei diesem würden nicht mehr die Personen direkt verpflichtet werden, sondern Unternehmen oder Organisationen müssten solche Identifizierungen durchführen. Die einzelne Person wird die Konsequenz nicht sofort erkennen. Jedoch wird sie sich, sobald sie auf die Dienstleistung einer derart regulierten Organisation zugreifen möchte, identifizieren müssen.[75]

74 Siehe Lessig, *Code*, S. 54. Parallel zur Identifizierbarkeit hat Kapitel 6 gezeigt, dass Überwachungsmaßnahmen zunehmend kostengünstiger werden und eine Aufwand-Ertrag-Abwägung immer mehr zugunsten der Seite der Überwachung ausfallen kann.

75 Kritisch äußert sich hier auch Kaye: „Such intermediary liability is likely to result either in real-name registration policies, thereby undermining anonymity, or the elimination of posting altogether by those websites that cannot afford to implement screening procedures, thus harming smaller, independent media." Kaye, *A/HRC/29/32*, para. 54.

In beiden Fällen, der direkten wie der indirekten Verpflichtung, ist die Konsequenz ähnlich: Die *digitale* Identität, die durch die kryptographische Authentifizierung nachgewiesen werden kann, wird mit der *realen* Identität verknüpft. Anders ausgedrückt handelt es sich um die Verbindung der *Offline*-Identität mit der *Online*-Identität. Moderne Kryptographie ist hierbei zentrales Mittel zum Zweck: Ab dem Zeitpunkt, an dem diese Verbindung zustande kommt, schaffen digitale Signaturen eine dauerhafte Zurückverfolgbarkeit zur persönlichen Identität. Eine Nutzerin oder ein Nutzer kann aus *mathematischen* Gründen die Herkunft seiner oder ihrer Nachricht nicht mehr abstreiten.[76]

Dies widerspricht nun der verbreiteten, aber unbegründeten Annahme, das Internet sei generell oder *by design* anonym.[77] Anonym war das Internet faktisch nur so lange, bis Unternehmen und Regierungen begannen, die technologischen Adressen (etwa IP-Adressen) mit persönlichen Identitäten zu verbinden.[78] Andy Greendberg greift dieses Problem auf und verdeutlicht die Gegensätze in der Wahrnehmung von Sicherheit im Internet wie folgt:

> Half of security gurus preach about the Internet's invasion of privacy, while the other half bemoan the Internet's lack of authentication, which they say makes the task of identifying bad actors – what they call the attribution problem – nearly impossible.[79]

Das *Going-Dark-Problem* aus Kapitel 6 schwingt hier unterschwellig mit. Letztlich haben jedoch beide Seiten recht. Was paradox scheinen mag, ist mit dem Wissen um die Grundprinzipien des Internets einfach zu erklären. Das Internet verlagert mit der Idee des Ende-zu-Ende-Prinzips Komplexität an den Rand des Netzwerks.[80] Nicht eine zentrale Instanz

76 Solove schreibt hierzu: „Identification is similar to aggregation as both involve the combination of different pieces of information, one being the identity of a person. However, identification differs from aggregation in that it entails a link to the person in the flesh." Solove, „A Taxonomy of Privacy", S. 512.

77 Siehe weiterführend Abschnitt 4.1.

78 So erkennt Edward Snowden bezogen auf die Entwicklung des Internets: „In the 1990s, the Internet had yet to fall victim to the greatest iniquity in digital history: the move by government and businesses to link, as intimately as possible, users' online personas to their offline legal identity." Snowden, *Permanent Record*, S. 46–47.

79 Greenberg, *This Machine Kills Secrets*, S. 6.

80 Siehe Lessig, *Code*, S. 44.

ist verantwortlich für die Sicherheit (oder jetzt eben: Anonymität, Privatsphäre etc.), sondern die Applikationen selbst sind es. Dies bedeutet zwar nicht, dass Applikationen *alles* machen können – schließlich müssen Protokolle zur gemeinsamen Kommunikation gefunden werden, und Standardisierungen erleichtern den Datenaustausch. Jedoch wird vieles an Verantwortung darüber auf die Applikationsebene übertragen, was dazu führt, dass einige Applikationen ein Maß an Sicherheit, Privatsphäre oder nun eben Anonymität gewährleisten – und andere nicht. Greenberg führt daher zu Recht weiter aus:

> Those who behave a certain way online and use certain services will have no privacy, while those who behave another way and use other services can be very, very hard to identify – harder to identify now, in many ways, than ever in communication history.[81]

Damit ist die Parallele zur egalitären Kryptographie aus Abschnitt 7.2 unübersehbar. Obgleich wir uns nun mit Anonymität beschäftigen (und nicht mehr mit vertraulicher Kommunikation), sind die gleichen Implikationen für Gleichheit und Ungleichheit auch hier erkennbar. Die Personen, die technologisch erfahren sind, die den Tor-Browser nutzen, die sich spezielle Software leisten können – all diese Personen werden auch bei Identifizierungsmaßnahmen Mittel und Wege finden, weiterhin *relativ* pseudonym im Internet agieren zu können. Den anderen aber, den gewöhnlichen Menschen, die weder über Technologiekompetenz noch über Kapital verfügen, bleibt diese Möglichkeit verwehrt. Anonymität ist die andere Seite der Medaille einer egalitären Kryptographie.

Darauf weist auch Lessig hin, wenn er feststellt, dass zumindest *für die meisten Menschen* Anonymität im Internet kaum mehr möglich sein wird.[82] Eine direkte wie auch eine indirekte Verpflichtung zur Identifizierung ist für *die meisten* umsetzbar, aber nicht zwangsläufig für alle. Diese Regulierungen betreffen in der Konsequenz stets den *Großteil* der Bevölkerung – vor allem die Menschen, die sich wenig mit solchen Fragen auseinandersetzen müssen oder wollen. Den Entscheiderinnen und Entscheidern über die Internet Policy und kryptographische Regulierung sollte stets bewusst sein, dass jede Entwicklung hin zu mehr KYC-Verfahren und weniger Möglichkeiten zur Anonymität zu Ungleichheiten führen

81 Greenberg, *This Machine Kills Secrets*, S. 7.
82 Siehe Lessig, *Code*, S. 54.

muss. Es darf dabei bezweifelt werden, dass Kriminelle oder das organisierte Verbrechen von solchen Praktiken abgeschreckt werden. Vielmehr werden sie stets Möglichkeiten suchen (und oftmals auch finden), die Verpflichtung zur Identifizierung zu umgehen. Eine egalitäre Kryptographie im Bereich der Identifizierung kann es nur geben, wenn es auch für Laien Möglichkeiten zur vertraulichen *und* anonymen Kommunikation gibt.

In diesem Sinne handelt es sich bei Identität und Authentizität tatsächlich um eine zwiespältige Angelegenheit: Einerseits besteht die technische Notwendigkeit der Schutzziele wie etwa der Authentifizierung, welche die Nutzbarkeit des Internets ermöglicht, wie wir es kennen; andererseits gibt es die Verknüpfung der Online- mit der Offline-Welt – wenn man vereinfacht davon ausgeht, dass eine solche Trennung überhaupt jemals möglich war. Diese Trennung verschwimmt durch eine omnipräsente Identifizierung, sei sie direkt durch Identifikationsmerkmale oder indirekt mit transitiver Authentifizierung. Während bei der Vertraulichkeit eine freie, zugängliche und tatsächlich genutzte Kryptographie notwendig ist, ist mit Blick auf die Identifikation aus normativer Perspektive Zurückhaltung geboten. David Kaye, damaliger UN-Sonderberichterstatter für Meinungsfreiheit, kommt im Kontext der Menschenrechte sogar zu dem Schluss, dass das Verbot der Anonymität in das Recht auf die Freiheit der Meinungsäußerung eingreift.[83] Mit Blick auf das Beispiel der SIM-Karten und der KYC-Verpflichtung schreibt Kaye weiter:

> Such policies directly undermine anonymity, particularly for those who access the Internet only through mobile technology. Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest.[84]

Aus ethischer Sicht sollte aber nicht nur aus menschenrechtlicher und konsequentialistischer Sicht Zurückhaltung geboten sein. Vielmehr ist auch das Konzept *Identität* und *Identifizierung* so uneindeutig, dass fraglich ist, ob es dauerhaft und omnipräsent mit kryptographischer Authentifizierung verbunden werden sollte. Dazu kann als ein letztes Beispiel das Thema der Staatsbürgerschaft betrachtet werden.[85] Digitale Identifizie-

83 Siehe Kaye, *A/HRC/29/32*, para. 49.

84 Ebd., para. 51.

85 Siehe zur geschichtlichen Einführung der Staatsbürgerschaft etwa Heater Derek. *A Brief History of Citizenship*. Edinburgh: Edinburgh University Press, 2004.

rung, etwa mit einem Ausweiszwang im Internet, kann heute die Verbindung von Identifikationsmerkmalen und Staatsbürgerschaft mithilfe kryptographischer Authentifizierung ermöglichen. Es ist jedoch daran zu zweifeln, ob eine solche Identifikation dem Menschen als komplexem, individuellem Wesen gerecht wird. In einer derart technologisierten Welt ist eine kritische Perspektive immer wieder neu gefordert. Gerade in Zeiten großer Migrationsbewegungen und gesamtgesellschaftlicher Abgrenzungserscheinungen ist der Drang nach Identifikation durch *harte* Identifikationsmerkmale wie Staatsbürgerschaft, Geschlecht oder Hautfarbe gefährlicher denn je.

Selbst wenn solche Identifikationsmerkmale mehrere Optionen zuzulassen scheinen, etwa eine diskrete Altersangabe oder unterschiedliche Staatsbürgerschaften, handelt es sich im praktischen Kern letztlich um *binäre Merkmale*: Willkommene Staatsbürgerschaft – ja oder nein. Passendes Geschlecht – ja oder nein. Arbeitsfähiges Alter – ja oder nein. Gerade weil diese Merkmale im Eigentlichen binär genutzt werden, dabei aber oftmals von den Betreffenden nicht gewählt wurden, handelt es sich um einen ungelösten Konflikt um Identifizierung und Anonymität. Auf einen solchen Konflikt weisen auch Diffie und Landau hin:

> Anonymity and identity are among the many threads in human culture that have existed in uneasy harmony for millennia. The revolutionary changes of the 1990s – globalization, mobility, greater availability of information – brought many of these threads into open conflict and a new balance among them has yet to be found.[86]

Die Gefahr des 21. Jahrhunderts wird sein, dass sich Gesellschaften innerhalb weniger Jahre auf Identifizierung stürzen und Anonymität brandmarken; dass all die philosophischen, ethischen und sozialen Fragen der Identifizierung bis dahin aber noch nicht abschließend ausgehandelt sein werden; und dass es letztlich kryptographische Methoden sein werden, die eine unausweichliche Identifizierung fast aller Menschen ermöglichen. Sei es durch mathematische Methoden, signierte Gesichtserkennung oder biometrische Merkmale. In jedem Fall wird das menschliche Individuum dann zum Ausdruck einer digitalen Signatur und einiger weniger Bits.

86 Diffie und Landau, *Privacy on the Line*, S. 275.

8 Synthese und Anwendung

> People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.
>
> – Eric Hughes in *A Cypherpunk's Manifesto*[1]

Die vorherigen Kapitel haben gezeigt, dass Kryptographie nicht bloß reine Technologie ist, sondern auch von ethischen und gesellschaftlichen Rahmenbedingungen abhängt. Diese Rahmenbedingungen werden zwar durch eine freie, zugängliche und egalitäre Kryptographie beeinflusst. Gleichzeitig wirken sie aber selbst auf die Kryptographie ein, darauf, wie wir mit der Möglichkeit der Kryptographie umgehen, wie wir sie nutzen und wie wir die Grundlagen schaffen, dass die Entwicklung der Kryptographie gefördert werden kann. In diesem letzten Kapitel soll eine anwendungsorientierte Perspektive eingenommen werden, um anhand von exemplarischen Situationen aufzuzeigen, wie relevant eine Ethik der Kryptographie in den aktuellen Entscheidungen ist. Damit handelt es sich um eine Synthese der technologischen Grundlagen aus Teil I, der gesellschaftlichen Faktoren aus Teil II und der ethischen Analyse aus dem bisherigen Teil III.

Auch wenn es eine Vielzahl von Anwendungsfällen gäbe, wird sich dieses Kapitel auf drei Fallbeispiele beschränken: auf das sogenannte *Client-Side-Scanning* (CSS), das erst durch das maschinelle Lernen und die massenhafte Datenverarbeitung möglich wurde (Abschnitt 8.1), auf die Bedeutung von Intermediären und die ethische Bewertung einer entsprechenden Regulierung (Abschnitt 8.2) und auf die Zukunft der Kryptographie, wobei insbesondere Ethik und Quantum Computing in ihrem Zusammenhang betrachtet werden (Abschnitt 8.3).

Das Kapitel schließt damit inhaltlich auch an Abschnitt 4.3 an: In der medialen Wahrnehmung könnte man den Eindruck gewinnen, als gäbe es kaum mehr Diskussionen um den richtigen Umgang mit Kryptographie.

1 Hughes, *A Cypherpunk's Manifesto*.

Allzu leicht kann dies zu der Annahme führen, dass die Crypto Wars der Vergangenheit angehören. Diese Einschätzung ist allerdings falsch. Die folgenden drei Abschnitte werden aufzeigen, dass neue Technologien, Versuche der intermediären Regulierung und das Quantum Computing gerade jetzt Teil eines Crypto Wars des 21. Jahrhunderts sind.[2]

8.1 Client-Side-Scanning (CSS)

Das erste Fallbeispiel der Ethik der Kryptographie beschäftigt sich primär mit dem Schutzziel der *Vertraulichkeit* und der Ende-zu-Ende-Verschlüsselung (E2E-Verschlüsselung). Die Ausgangslage und Grundproblematik sei dabei die Folgende: Die verschlüsselte Kommunikation sei *so gut*, dass eine Entschlüsselung für Drittparteien selbst dann nicht möglich sei, wenn *sehr gute* Gründe sie rechtfertigen würden – wenn es beispielsweise um das Recht auf Leben oder den Schutz von Minderjährigen gehe. Daher sei eine Möglichkeit zu schaffen, die verschlüsselte Kommunikation *trotzdem* technologisch zu entschlüsseln. Das müsse üblicherweise über die Intermediäre erfolgen.

Wenn wir ein solches Fallbeispiel genauer untersuchen, sind drei Aspekte zu unterscheiden: (I) die inhaltliche Grundannahme, dass Entschlüsselung *überhaupt* nicht mehr möglich ist, insofern die Algorithmen nicht zu brechen sind; (II) die normative Aussage, dass dies in Situationen mit *sehr guten* Gründen trotzdem möglich sein sollte; (III) die prozedurale Umsetzung, bei der die Regulierung nicht direkt beim Individuum ansetzt, sondern bei den Intermediären. Aufgrund der Verallgemeinerbarkeit der prozeduralen Umsetzung wird (III) im nachfolgenden Abschnitt behandelt. Die beiden anderen Aspekte (I) und (II) sind im Folgenden zunächst generell und anschließend bezogen auf das Client-Side-Scanning (CSS) zu analysieren.

Zunächst zur Grundannahme (I): Kapitel 6 hat bereits gezeigt, dass sich viele konsequentialistische Dichotomien letztlich als *Schein*-Dichoto-

2 Auch Craig Jarvis sieht einen *dritten* Crypto War ab 2013. Er bezieht sich jedoch insbesondere auf den US-amerikanischen Kontext, das Wirken des FBI und die Snowden-Veröffentlichungen; siehe Jarvis, *Crypto Wars*, S. 319–404. Die folgenden Abschnitte werden eine andere Schwerpunktsetzung vornehmen und knüpfen den dritten (oder je nach Definition auch vierten) Crypto War an das Client-Side-Scanning und das Quantum Computing.

mien erweisen. Insbesondere ist hier die bipolare Vorstellung von *Privacy vs. Sicherheit* und *Überwachung vs. Kryptographie* zu nennen. Aber auch das damit zusammenhängende *Going-Dark-Problem*, bei dem davon ausgegangen wird, dass Strafverfolgungsbehörden keinen Zugriff mehr auf Kommunikationsdaten bekommen können, entspricht nicht der technologischen Realität. Wir können an dieser Stelle zwei Gründe rekapitulieren, die entschieden gegen ein solches Argument sprechen.

Einerseits ist die Annahme falsch, dass eine Entschlüsselung der Kommunikation *unter keinen Umständen* mehr möglich ist. Zwar lässt sich ein Algorithmus wie AES nicht mathematisch brechen, doch muss an irgendeiner Stelle der Schlüssel gespeichert werden. Im Falle von *Public-Key Infrastructures* (PKI), die eine authentifizierte E2E-Verschlüsselung ermöglichen, ist ebenfalls ein Schlüssel auf den Endgeräten der Nutzerinnen und Nutzer vorhanden. Mit einem physischen Zugriff auf die Endgeräte ist eine Entschlüsselung des Kommunikationsverlaufs gegebenenfalls doch und viel zielgerichteter möglich. Hinzu kommen in der Praxis bereits eingesetzte Methoden wie Staatstrojaner (etwa *Pegasus*), die eine Überwachung *trotz* Verschlüsselung erlauben.[3]

Andererseits ist auch die weitere Annahme falsch, dass *ausschließlich* die inhaltlichen Kommunikationsdaten zur Informationsgewinnung dienlich sind. Auch sogenannte *Metadaten* spielen hier eine entscheidende Rolle. Dies sind Daten, die zur Kommunikation erforderlich sind, aber nicht den Inhalt der Kommunikation übertragen. Beispielsweise handelt es sich darum, wann und mit wem kommuniziert wurde. Gerade in Fällen des organisierten Verbrechens und bei größeren Strukturen können solche Metadaten zur Informationsgewinnung hilfreich sein. Der Einsatz von E2E-Verschlüsselung verhindert die Ansammlung von Metadaten nicht per se. Ausgenommen davon sind zwar Technologien wie das Tor-Netzwerk, das *auch* Metadaten verschleiern kann. Allerdings zielen aktuelle Regulierungsversuche nicht explizit darauf ab.

Zusammenfassend ist also bereits die Grundannahme des Going-Dark-Problems kritisch zu hinterfragen. Das hat Auswirkungen auf die normative Aussage (II), nach der ein Zugriff auch ohne Schlüssel in bestimmten Situationen möglich sein sollte. Um die Überzeugungskraft die-

3 Dies bedeutet in normativer Hinsicht nicht automatisch, dass Staatstrojaner legitim sind. Um diese Frage zu beantworten, bedarf es allerdings einer eigenen Untersuchung. Zur Spionagesoftware Pegasus der NSO Group siehe Richard und Rigaud, *Pegasus*.

ser Aussage zu untersuchen, sind zunächst die verschiedenen normativen Alternativen zu betrachten. So sprechen sich etwa Kardefelt-Winther u. a. im UNICEF Research Working Paper *Encryption, Privacy and Children's Right to Protection from Harm* aus dem Jahr 2020 dafür aus, polarisierte und absolute Positionen im Bereich der E2E-Verschlüsselung abzulehnen:

> The debate around end-to-end encryption of digital communications has been polarized into absolutist positions. These include advocating 1) for the unlimited use of end-to-end encryption; 2) for the complete abolishment of end-to-end encryption; and 3) that law enforcement should always be able to access encrypted data and will be unable to protect the public unless it can do so. Such polarized positions ignore the complexity and nuance of the debate and act as an impediment to thoughtful policy responses.[4]

Betrachten wir die einzelnen, scheinbar *absoluten* Positionen etwas genauer. Position 2, der zufolge die E2E-Verschlüsselung vollständig abgeschafft werden soll, dürfte zunächst kaum jemand mehr einnehmen. Selbst ein autokratisch regiertes Land oder ein profitorientiertes Unternehmen hat kein Interesse daran, die E2E-Verschlüsselung gänzlich zu verbieten. Viel zu groß wären gerade in einer hochtechnologisierten Welt die Gefahren, die von einer unverschlüsselten Kommunikation und Datenspeicherung ausgehen würden. Einerseits kann man hier an nationale Interessen im internationalen Wettbewerb denken, andererseits aber auch an sehr praktische Fragen der öffentlichen Sicherheit, zum Beispiel der Kommunikation im Gesundheitswesen oder bei Finanztransaktionen.

Position 3 ist jene Variante, die am meisten diskutiert wird, wenn es um eine Art Trade-off von Privacy vs. Sicherheit gehen soll. Gebietet es das Gesetz, gegebenenfalls auch unter dem Vorbehalt der richterlichen Zustimmung, dann soll ein Zugriff der Strafverfolgungsbehörden auf die Daten möglich sein. Dieser Position liegt somit der Wunsch nach einem *legalen und legitimen* Zugriff auf verschlüsselte Kommunikation zugrunde. Man könnte dies auch als den Wunsch nach *nur ein bisschen* Kryptographie beschreiben – nämlich genau so viel, dass das unbescholtene Individuum verschlüsselt kommunizieren kann, Kriminelle jedoch nicht.

Position 3 kann allerdings *per definitionem* nicht umgesetzt werden. Das Prinzip der E2E-Verschlüsselung basiert darauf, dass keine Partei auf

4 Kardefelt-Winther u. a., *Encryption, Privacy and Children's Right to Protection from Harm*, S. 3.

den Inhalt zugreifen kann außer die Kommunizierenden selbst respektive deren Geräte. Die Vorstellung von einer Technologie, die einerseits den Zugriff auf die verschlüsselte Information erlaubt, andererseits aber auch die Wahrung der E2E-Verschlüsselung gestattet, ist aus logischer Sicht per definitionem falsch. Dazu kann auch kein *Mittelweg* oder *Kompromiss* gefunden werden, der die beiden sich gegenseitig ausschließenden Eigenschaften (Zugriffsmöglichkeit *und* E2E-Verschlüsselung) verbinden würde. Bisherige Versuche wie beispielsweise der Clipper-Chip, der bereits in Kapitel 4 diskutiert worden ist, konnten daher nur scheitern. Wenn die E2E-Verschlüsselung nicht nur all die Vorteile bietet, die in Kapitel 6 besprochen worden sind, sondern auch aus Menschenrechtsperspektive geboten ist, dann *muss* ein solcher Versuch auch aus ethischer Perspektive abgelehnt werden. Eine Alternative zu Position 1, bei der eine freie, unbeschränkte und ubiquitäre Kryptographie geboten ist, ist bislang nicht ersichtlich. Betont werden muss dabei erneut, dass Position 1 *nicht* bedeutet, dass unter keinen Umständen eine Entschlüsselung oder ein Zugriff auf die Daten möglich ist. Auch hier ist die Kryptographie keine hinreichende Bedingung zur Vertraulichkeit.[5]

Zwar scheint es, als wäre die Sachlage damit eindeutig. Nun gibt es allerdings eine Technologie, die einen Trade-off *doch noch* ermöglichen will, die *doch noch* Position 1 ablehnen kann, die *doch noch* eine vierte Position erlauben soll. Dieser Versuch ist das sogenannte *Client-Side-Scanning* (CSS). Das CSS ist insofern von hoher Relevanz, als es seit 2020 in verschiedenen Ländern auf der Welt im Kontext des Kinderschutzes diskutiert wird. Insbesondere in der Europäischen Union, dem Vereinigten Königreich sowie den USA wurden Gesetze vorgeschlagen, die das CSS in unterschiedlicher Ausprägung für manche Kommunikationsdienstleister verpflichtend machen würden.[6] Von Bürgerrechtsorganisationen und

5 Die im Allgemeinen ausgewogene und differenzierte Diskussion bei Kardefelt-Winther u. a. kommt wohl auch deshalb nicht zu einem Ergebnis, weil Position 1 strikt abgelehnt wird. Es wird vielmehr davon gesprochen, dass Menschenrechtsorganisationen eine „nuanced position on encryption and possible technological and legal solutions" übernehmen sollten. Es bleibt aber weitgehend unklar, wie eine „nuanced position" aussehen könnte. Aus Perspektive der hier vorgestellten Ethik der Kryptographie ist ein Nuancieren von Position 1 nicht absehbar. Ebd., S. 12, siehe auch S. 12–13 sowie S. 3. Die von ihnen zitierte und empfohlene Carnegie-Endowment-Arbeitsgruppe kommt hier jedoch zu technisch nachvollziehbaren Lösungen; siehe Encryption Working Group, *Moving the Encryption Policy Conversation Forward*.

6 Siehe Markus Reuter. „Gesetzesvorhaben in EU, UK und den USA gefährden Verschlüsselung". In: *Netzpolitik.org* (2022). URL: https://netzpolitik.org/2022/crypto-

zahlreichen Medien im deutschsprachigen Raum wird die Technologie des CSS auch als *Chatkontrolle* bezeichnet.[7] Doch welche Möglichkeiten, Gefahren und Probleme würde ein solches CSS mit sich bringen? Warum wird von manchen das CSS als Lösung dafür verstanden, Sicherheit mit dem Recht auf Privacy und verschlüsselter Kommunikation zu verbinden? Ermöglicht das CSS doch die Verbindung von E2E-Verschlüsselung und partieller Zugriffsmöglichkeit?

Zur Beantwortung dieser Fragen betrachten wir zunächst die technologische Funktionsweise.[8] Die entscheidende Idee beim CSS ist, eine Analyse der Nachrichten oder Bilder nicht mehr *serverseitig* durchzuführen. Die Kommunikation über den Server kann daher tatsächlich verschlüsselt stattfinden. Eine Analyse soll aber *clientseitig* stattfinden, also auf dem Endgerät der Nutzenden.[9] Analog kann man dies auf stark vereinfachte Weise mit einem Briefversand verdeutlichen: Zunächst wird von der Absenderin oder dem Absender ein Text auf einem Blatt Papier verfasst. *Bevor* das beschriebene Blatt in ein Kuvert verpackt wird, wird der Text auf gewisse Merkmale und Kriterien hin untersucht. Erst *danach* wird das Blatt in das Kuvert verpackt, versiegelt und übermittelt.[10] Im Schritt der maschinellen Analyse wird – wenn ein Treffer nach bestimmten Kriterien

wars-gesetzesvorhaben-in-eu-uk-und-den-usa-gefaehrden-verschluesselung (besucht am 15.04.2024). Diese internationale Dimension ist im Rahmen der Kryptographie nicht neu. Im Kontext des *Communications Assistance for Law Enforcement Act* (CALEA) von 1994, der eine Ausweitung der Überwachung durch Strafverfolgungsbehörden ermöglicht hatte, gab es ähnliche Vorschläge auch in der Europäischen Union und in Großbritannien; siehe Diffie und Landau, *Privacy on the Line*, S. 224–226.

7 Siehe z. B. Kathrin Schmid. „Im Dilemma zwischen Daten- und Kinderschutz". In: *Tagesschau* (14. Nov. 2023). URL: https://www.tagesschau.de/ausland/europa/chatkontrolle-eu-kindesmissbrauch-100.html (besucht am 15.04.2024); oder Meike Laaff. „Wir haben ja nichts gegen Verschlüsselung. Aber". In: *ZEIT Online* (12. Mai 2022). URL: https://www.zeit.de/digital/2022-05/chatkontrolle-eu-kinder-sexualisierte-gewalt-chatverschluesselung-datenschutz (besucht am 15.04.2024); im Englischen auch Morgan Meaker. „Europe's Moral Crusader Lays Down the Law on Encryption". In: *Wired* (11. Mai 2023). URL: https://www.wired.co.uk/article/europes-ylva-johansson-lays-down-the-law-on-encryption (besucht am 15.04.2024).

8 Siehe einführend und zur folgenden technologischen Beschreibung Abelson u. a., *Bugs in our Pockets*.

9 Abelson u. a. unterscheiden auch zwischen einer privaten Sphäre als Client und einer öffentlichen Sphäre; siehe ebd., S. 5–6 sowie S. 11.

10 Zur Vereinfachung gehen wir davon aus, dass niemand bis auf die empfangende Partei den Brief öffnen kann.

erfolgt ist – der Inhalt des Briefes an eine Drittpartei (etwa eine Strafverfolgungsbehörde) gesendet.

Das CSS funktioniert methodisch nicht viel anders: Vor dem Versenden einer E-Mail oder einer Nachricht wird ihr Inhalt zunächst analysiert. Technologisch betrachtet erfolgt dies entweder mit Hashverfahren oder per maschinellem Lernen.[11] Erst im Anschluss wird die Nachricht verschlüsselt und per E2E-Verschlüsselung übermittelt. Wird sie im Analyseprozess nach bestimmten Kriterien (etwa im Sinne der Terrorismusbekämpfung) markiert, kann sie an eine Drittpartei gesendet werden. Auf den ersten Blick scheint es, als könnte damit einerseits einem Kontrollbedürfnis oder -erfordernis Genüge getan, andererseits aber auch die E2E-Verschlüsselung ermöglicht werden. Allerdings gibt es hier entscheidende ethische und technologische Gründe, die gegen die Implementierung eines CSS sprechen.[12]

Zunächst sind Missverständnisse um das CSS auszuräumen: Eine vollständige Vertraulichkeit und die Intention der E2E-Verschlüsselung ist beim CSS nicht gewahrt.[13] Dies wäre ausschließlich dann gegeben, wenn die Nachricht möglichst direkt nach dem Klick auf „Absenden" bis zum Zeitpunkt der Ankunft in der empfangenden Applikation verschlüsselt wäre und keine andere Partei sie entschlüsselt lesen könnte. Beim CSS besteht jedoch die Möglichkeit, dass Nachrichten an andere Parteien als die Zielpartei gesendet werden (etwa Strafverfolgungsbehörden). Per definitionem soll mit Vertraulichkeit und E2E-Verschlüsselung aber gerade verhindert werden, dass eine Drittpartei auch auf nur *eine* Nachricht zugreifen kann. Von E2E-Verschlüsselung im Kontext des CSS zu sprechen, ist daher irreführend.

Nun könnte es als akzeptabel erscheinen, dass die Idee der E2E-Verschlüsselung nicht mehr vollständig gegeben ist. Es wäre dann von einer *partiellen* Vertraulichkeit zu sprechen. Doch auch in diesem

11 Siehe ebd., S. 7–8.

12 Siehe zur technischen Bewertung ebd.

13 Siehe im Kontext des Hashing und des Client-Side-Scanning Erica Portnoy. *Why Adding Client-Side Scanning Breaks End-To-End Encryption*. Electronic Frontier Foundation. 1. Nov. 2019. URL: https://www.eff.org/de/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption (besucht am 15.04.2024). Zur Definition der E2E-Verschlüsselung siehe etwa Mohamed Nabeel. „The Many Faces of End-to-End Encryption and Their Security Analysis". In: *IEEE International Conference on Edge Computing (EDGE)*. 2017, S. 252–259; sowie Macnish, „An End to Encryption?"

Fall sind zahlreiche Gründe gegen das CSS anzuführen. Technologisch betrachtet schafft das CSS mit einer solchen *partiellen* Vertraulichkeit zunächst nicht *mehr*, sondern *weniger* digitale Sicherheit. Die einflussreichen und renommierten Kryptographinnen und Kryptographen Abelson u. a. zeigen in ihrem Artikel *Bugs in our Pockets: The Risks of Client-Side Scanning* überzeugend auf, wie das CSS eine Gefahr für die Informationssicherheit darstellt:

> Although CSS is represented as protecting the security of communications, the technology can be repurposed as a general mass-surveillance tool. The fact that CSS is at least partly done on the client device is not, as its proponents claim, a security feature. Rather, it is a source of weakness. As most user devices have vulnerabilities, the surveillance and control capabilities provided by CSS can potentially be abused by many adversaries, from hostile state actors through criminals to users' intimate partners. Moreover, the opacity of mobile operating systems makes it difficult to verify that CSS policies target only material whose illegality is uncontested.[14]

Diese Reduktion *digitaler* und in der Konsequenz *allgemeiner* Sicherheit hängt mit der Gefahr falsch-positiver Meldungen zusammen. Einerseits sind sogenannte *false-positive attacks* möglich.[15] Andererseits widerspricht jede falsch-positive Meldung der Idee von Privacy: Bei Milliarden Nachrichten, die täglich gesendet werden, würde selbst eine niedrige Falsch-Positiv-Rate genügen, dass Millionen dieser Inhalte an eine Drittpartei gemeldet werden.[16] Auch wenn die Rate gering scheint, handelt es sich doch um einen massiven Eingriff in die Privatsphäre zahlreicher Nut-

14 Abelson u. a., *Bugs in our Pockets*, S. 2. Die letzte Aussage verweist gerade auch auf die Möglichkeit des Missbrauchs, die im Folgenden beschrieben wird.

15 Siehe ebd., S. 28–30.

16 Siehe Andreas H. Woerlein. „EU-Kommission: Gesetzesvorschlag im Kampf gegen Kindesmissbrauch – kommt die Chatkontrolle?" In: *ZD-Aktuell* 01251 (2022); Wissenschaftliche Dienste des Deutschen Bundestages. *„Chatkontrolle" – Analyse des Verordnungsentwurfs 2022/0155 (COD) der EU-Kommission*. WD 10 – 3000 – 026/22. 2022. URL: https://www.bundestag.de/resource/blob/914580/9eba1ff3a5daa7708fca92e3184a1ae3/WD-10-026-22-pdf-data.pdf (besucht am 15.04.2024), S. 18; sowie Ulrich Kelber. *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestages am Mittwoch, 1. März 2023, 14:00 bis 16:00 Uhr zum Thema „Chatkontrolle"*. 28. Feb. 2023. URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_Chatkontrolle.pdf?__blob=publicationFile&v=1 (besucht am 15.04.2024), S. 2 sowie S. 10–11.

zerinnen und Nutzer. Jede einzelne falsch-positive Meldung zeigt, dass eine E2E-Verschlüsselung *de facto* nicht mehr vollständig gegeben ist.

In diesem Kontext kommt auch eine statistische Frage hinzu: Wer entscheidet über die Festlegung der statistischen Spezifität respektive Sensitivität? Durch solche Entscheidungen ist dem CSS eine Gefahr inhärent, die als Missbrauchspotential beschrieben werden kann.[17] Um diesen Aspekt exemplarisch zu verdeutlichen: Gehen wir davon aus, dass das CSS als Prävention gegen Kindesmissbrauch eingesetzt werden soll. Die Anbieter von Kommunikationsdienstleistungen müssen somit das CSS in ihren Applikationen implementieren – nach den Vorgaben und Kriterien des Gesetzes oder gar einer Exekutiv-Institution. Da es sich bei der Analyse des betreffenden Materials um maschinelles Lernen handelt, ist eine transparente Überprüfung der Methoden und der algorithmischen Entscheidungen erschwert.[18] Auch im Falle des Abgleichs von Hashwerten ist ein Machtmissbrauch möglich, insofern eine Veränderung auf einfache und intransparente Weise umsetzbar wäre, etwa zur Inklusion von Drogendelikten oder Gefährdungen nationaler Sicherheit. Im Kontext der Diskussion um die Chatkontrolle in der EU sprachen sich noch vor einer möglichen Verabschiedung des Gesetzes einzelne Abgeordnete sowie Europol für eine Ausweitung des zu untersuchenden Materials aus.[19] Auch nach Meinung der Wissenschaftlichen Dienste des Deutschen Bundestages wäre „eine Ausweitung der Überwachung auch auf andere Bereiche möglich und zu befürchten“[20].

17 Siehe Woerlein, „EU-Kommission: Gesetzesvorschlag im Kampf gegen Kindesmissbrauch – kommt die Chatkontrolle?“; sowie Wissenschaftliche Dienste des Deutschen Bundestages, „*Chatkontrolle*“, S. 19. Siehe auch Kelber, *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*, S. 3.

18 Zwar hat sich in den letzten Jahren einiges im Bereich des *erklärbaren/interpretierbaren maschinellen Lernens* (engl. *explainable AI*) getan, allerdings ist fraglich, ob diese Lösung auch im Fall des CSS ausreichende Kontroll- und Überwachungsmöglichkeiten zu bieten vermag. Siehe einführend zu *explainable AI* Dang Minh u. a. „Explainable artificial intelligence: a comprehensive review“. In: *Artificial Intelligence Review* 55.5 (2022), S. 3503–3568; aus historischer Perspektive auch Roberto Confalonieri u. a. „A historical perspective of explainable Artificial Intelligence“. In: *WIREs Data Mining and Knowledge Discovery* 11.1 (2021), e1391.

19 Siehe Andre Meister. „Politiker fordern Ausweitung der Chatkontrolle auf andere Inhalte“. In: *Netzpolitik.org* (6. Okt. 2023). URL: https://netzpolitik.org/2023/ueberwachung-politiker-fordern-ausweitung-der-chatkontrolle-auf-andere-inhalte (besucht am 15.04.2024).

20 Wissenschaftliche Dienste des Deutschen Bundestages, „*Chatkontrolle*“, S. 19.

Es ist auch davon auszugehen, dass das implementierte CSS nicht nur von demokratisch regierten Ländern genutzt würde. In westlich-liberalen Nationen entwickelte und eingesetzte Technologien ähneln denen in illiberalen Ländern zwar nicht im Inhalt, aber doch in ihrer Methodik.[21] Schon vor der Popularität des CSS brachte der Cypherpunk Jakob Appelbaum diese Problematik auf den Punkt: „We're building the same kind of authoritarian control structures, which will attract people to abuse them, and that's something that we try to pretend is different in the West."[22] Auch beim CSS scheinen demokratische Staaten den internationalen Aspekt zu vernachlässigen. Denn sobald das CSS einmal eingesetzt wird, ist es wahrscheinlich, dass autokratische Länder die Kriterien der Detektion gemäß ihren illiberalen, antidemokratischen und totalitären Vorstellungen anpassen werden. Das Missbrauchspotential erhält damit eine globale Komponente. Auch Volker Türk, der Hohe Kommissar der Vereinten Nationen für Menschenrechte, sieht eine besondere Gefahr durch das CSS in Regionen, in denen die Menschenrechte bedroht sind:

> In particular, where the rule of law is weak and human rights are under threat, the impact of client-side screening could be much broader, for example it could be used to suppress political debate or to target opposition figures, journalists and human rights defenders.[23]

Damit widerspricht das CSS dem Menschenrecht auf Meinungsfreiheit, Privacy und verschlüsselte Kommunikation. So sieht etwa der EU-Verordnungsentwurf nach Meinung der Wissenschaftlichen Dienste des Deutschen Bundestages „unverhältnismäßige Eingriffe in die geprüften Grundrechte der GRCh [Charta der Grundrechte der Europäischen Union] vor"[24]. Es ist zu erwarten, dass schon das bloße Wissen um die Möglichkeit eines staatlichen und/oder unternehmerischen Zugriffs auf

21 Siehe bezogen auf den Cyberspace und das Internet Matthias Schulze. „From Cyber-Utopia to Cyber-War: Normative Change in Cyberspace". Dissertation. Jena, 2018, S. 18–20. Gleiches lässt sich auch auf die Beschränkung und Regulierung von Kryptographie anwenden.

22 In Assange u. a., *Cypherpunks*, S. 130.

23 Volker Türk. *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*. A/HRC/51/17. United Nations Human Rights Council, 2022, para. 28.

24 Wissenschaftliche Dienste des Deutschen Bundestages, *„Chatkontrolle"*, S. 19.

Nachrichten zu einer Art Selbstzensur führen und so einen *chilling effect* zur Folge haben wird.[25]

Das CSS ist in diesem Sinne weniger *innovativ*, als es scheinen könnte. Es handelt sich um die gleiche Überwachungsmechanik und Beschränkung von kryptographischer Nutzung, wie sie in den vorangehenden Kapiteln diskutiert worden ist. Diese Überwachungstechnologie ist potentiell sogar *noch umfangreicher*, als ein Backdoor der Kommunikation es sein könnte. Bei einer Implementierung auf der Ebene des Betriebssystems ermöglicht das CSS ein Scanning des *gesamten* Endgeräts – und nicht nur der privaten Kommunikation mit anderen Parteien.[26] So kann es kaum überraschen, dass auch Volker Türk das CSS aus der Menschenrechtsperspektive grundsätzlich kritisiert. Türk bezieht sich dabei insbesondere auf die Risiken und die zu befürchtenden Konsequenzen:

> Given the broad range of significant risks to human rights protection from mandated general client-side screening, such requirements should not be imposed without further substantial consideration of their potential human rights impacts and measures that mitigate those harms. Without in-depth investigation and analysis, it seems unlikely that such restrictions could be considered proportionate under international human rights law, even when imposed in pursuit of legitimate aims, given the severity of their possible consequences.[27]

Im Sinne der angesprochenen Verhältnismäßigkeit (engl. *proportionality*) ist auch unklar, wie zielführend das CSS in der Praxis wirklich sein kann. Die Möglichkeiten von Attacken, die Rate an falsch-positiven Meldungen sowie die wenig ausgereiften technischen Lösungen lassen Zweifel an einem erfolgreichen Einsatz aufkommen. Auch für die Wissenschaftlichen Dienste des Deutschen Bundestages ist „fraglich, ob der aktuelle Verordnungsentwurf [der EU-Kommission] für das bezweckte Vorhaben überhaupt einen Mehrwert darstellt“[28]. Damit ist hinsichtlich der Erfül-

25 Siehe Kelber, *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*, S. 9 sowie S. 11. Siehe zum *chilling effect* allgemeiner auch Abschnitt 5.2; einführend dazu z. B. Büchi, Festic und Latzer, „The Chilling Effects of Digital Dataveillance“.

26 Siehe Abelson u. a., *Bugs in our Pockets*, S. 21–22.

27 Türk, *A/HRC/51/17*, para. 28. Neben den Ansichten des Europäischen Gerichtshofes werden hier zudem Volker Türk. *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*. A/HRC/39/29. United Nations Human Rights Council, 2018, para. 20, sowie Kaye, *A/HRC/29/32*, para. 43, zitiert.

28 Wissenschaftliche Dienste des Deutschen Bundestages, „*Chatkontrolle*“, S. 19.

lung des Prinzips der Verhältnismäßigkeit Skepsis geboten. Auch für den Wissenschaftlichen Dienst des Europäischen Parlaments verfehlt der europäische Vorschlag zum CSS diese Verhältnismäßigkeit:

> [N]ew binding obligations stemming from detection orders for relevant service providers to detect, report, and remove new material and grooming from their services would likely fail the proportionality test. In addition, in relation to the technology used regarding the detection of CSAM in E2EE communications, the device side scanning of interpersonal communications is disproportionate to the aims pursued.[29]

Zu einem ähnlichen Schluss kommt auch der Juristische Dienst des Rates der Europäischen Union. Er betont in seiner Begründung den *allgemeinen* und *unterschiedslosen* Zugriff auf den Inhalt persönlicher Kommunikation:

> [T]here is a serious risk of non-compliance with the principle of proportionality in so far as the detection orders would require the *general and indiscriminate access* to the content of personal communications by a specific service provider, and would apply without any distinction to all the persons using that specific service, without those persons being, even indirectly, in a situation liable to give rise to criminal prosecution.[30]

Im Sinne der Verhältnismäßigkeit ist zu bedenken, dass verschlüsselte Kommunikation niemals *gänzlich* unterdrückt oder verboten werden kann. In diesem Punkt haben die Cypherpunks vollkommen recht. All die Algorithmen sind bereits öffentlich zugänglich, und es scheint wenig wahrscheinlich, dass idealistische Open-Source-Entwicklerinnen und -Entwickler das CSS in ihre Software implementieren würden. Auf der anderen Seite haben aber gerade Kriminelle ein Interesse daran, weiterhin verschlüsselt kommunizieren zu können. Die naheliegende Folge wäre, dass die breite Bevölkerung de facto einer Überwachung ausgesetzt wäre,

29 European Parliamentary Research Service. *Proposal for a regulation laying down the rules to prevent and combat child sexual abuse: Complementary impact assessment*. PE 740.248. 2023. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf (besucht am 15.04.2024), S. VII.

30 Legal Service of the Council of the European Union. *Opinion of the Legal Service*. 8787/23. 26. Apr. 2023. URL: https://data.consilium.europa.eu/doc/document/ST-8787-2023-INIT/en/pdf (besucht am 15.04.2024), para. 66, zur Verhältnismäßigkeit para. 59–76, kursiv im Original.

Kriminelle aber aufgrund der Bedeutung von Verschlüsselung auf quelloffene und sichere Alternativen ausweichen dürften. Oder in den bekannten Worten von Phil Zimmermann: „If privacy is outlawed, only the outlaws will have privacy."[31] Diese Konsequenz würde einer egalitären Kryptographie fundamental widersprechen.

Mit Blick auf das Konzept einer egalitären Kryptographie ist auch beim CSS zu fragen, wie damit hochsensible Daten und Geheimdokumente versendet werden sollen. Sollen auch sie von den Dienstleistern gescannt werden? Sollen hierfür andere Regelungen gelten? Soll es erlaubt sein, andere Messengerdienste zu nutzen? Bezogen auf den EU-Verordnungsentwurf wurde daher von der damaligen spanischen Ratspräsidentschaft eingefügt, dass nicht-öffentliche Messengerdienste bei Fragen nationaler Sicherheit exkludiert werden sollten.[32] Nicht abwegig scheint es, dass selbst die Befürworterinnen und Befürworter des Gesetzes um die Lücken dieser Technologie wissen und daher bestimmte Bereiche ausnehmen wollen – wäre das CSS so sicher und so erfolgreich wie erhofft, wäre eine solche Differenzierung kaum notwendig. Eine Unterscheidung von Themen nationaler Sicherheit (oder Ähnlichem) einerseits und der Kommunikation von Individuen andererseits konterkariert die Idee einer egalitären Kryptographie, für die Abschnitt 7.2 argumentiert hat.

Die bisher betrachteten Argumente sprechen als Synthese von Technologie und Ethik gegen den Einsatz des CSS. Im Kontext der EU-weiten Chatkontrolle kam jedoch Kritik nicht nur von Bürgerrechtsbewegungen und aus der Zivilgesellschaft, sondern in Teilen auch von Kinderschutzorganisationen.[33] Denn kritisch zu bedenken ist beim CSS, dass Sicherheit im Internet und in der Kommunikation *auch* Minderjährige, vulnerable Bevölkerungsgruppen und Minderheiten schützen kann.[34] Um ein Bei-

31 Zimmermann, *Why I Wrote PGP*.

32 Siehe Andre Meister. „EU-Rat verschiebt Abstimmung über Chatkontrolle". In: *Netzpolitik.org* (21. Sep. 2023). URL: https://netzpolitik.org/2023/internes-protokoll-eu-rat-verschiebt-abstimmung-ueber-chatkontrolle/ (besucht am 15.04.2024).

33 Siehe Franziska Rau und Esther Menhard. „Wie die Chatkontrolle EU-weit Wellen schlägt". In: *Netzpolitik.org* (15. Sep. 2022). URL: https://netzpolitik.org/2022/plaene-der-kommission-wie-die-chatkontrolle-eu-weit-wellen-schlaegt/ (besucht am 15.04.2024); sowie Sebastian Meineck. „Das sagen Kinderschutz-Organisationen zur Chatkontrolle". In: *Netzpolitik.org* (20. Mai 2022). URL: https://netzpolitik.org/2022/massenueberwachung-das-sagen-kinderschutz-organisationen-zur-chatkontrolle (besucht am 15.04.2024).

34 Siehe Kardefelt-Winther u. a., *Encryption, Privacy and Children's Right to Protection from Harm*, S. 3.

spiel zu nennen: Im Kontext des vorgeschlagenen CSS wäre auch die digitale Kommunikation mit professionellen Jugendpsychologinnen oder -psychologen nicht mehr ungescannt möglich. Nicht nur wäre die Schweigepflicht dadurch de facto verletzt.[35] Auch würden Psychologinnen und Psychologen in den falschen Verdacht geraten, strafbare Handlungen durchzuführen.[36] Ein Algorithmus kennt weder Kontext noch Vergangenheit der nicht-digitalen Umwelt und wird daher einen tatsächlich relevanten Vorfall von einem nicht relevanten nur schwer unterscheiden können.[37]

Damit ist noch einmal auf die Analyse in Abschnitt 6.3 zurückzukommen. Unabhängig vom CSS weist bereits Daniel J. Solove im Kontext des *Nothing-to-hide-Arguments* auf eine ähnliche Begründung hin. Gesammelte Daten können zu einer *Verzerrung* führen, die niemals die ganze Person zu reflektieren vermag:

> Yet another problem with government gathering and use of personal data is *distortion*. Although personal information can reveal quite a lot about people's personalities and activities, it often fails to reflect the whole person. It can paint a distorted picture, especially since records are reductive – they often capture information in a standardized format with many details omitted.[38]

CSS ist eine Technologie, die ohne Kontext, Hintergrund und Zusammenhang oftmals zu einer solchen Verzerrung führt.[39] Doch gibt es Alternativen? Nach Ansicht von Ulrich Kelber, dem damaligen deutschen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, wären etwa niederschwellige Meldewege und die Förderung der Prävention sinnvoller und zielgerichteter.[40] An zahlreichen Stellen wurde zudem eruiert, dass einerseits Beschlagnahmungen der Endgeräte durch die

35 Siehe Kelber, *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*, S. 8–9.

36 Siehe allgemein zu falsch-positiven Meldungen ebd., S. 10–11.

37 Dass die deutsche *Tagesschau* dessen ungeachtet ein „Dilemma zwischen Daten- und Kinderschutz" konstruieren will, ist diskussionswürdig; siehe Schmid, „Im Dilemma zwischen Daten- und Kinderschutz".

38 Solove, *Nothing to Hide*, S. 28, kursiv im Original.

39 Würden allerdings Kontext, Hintergrund und Zusammenhang *auch* inkludiert, beispielsweise per Altersverifikation oder Berufshintergründen, ist von einer noch umfassenderen Überwachung auszugehen.

40 Siehe Kelber, *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit*, S. 12.

Strafverfolgung möglich sind und andererseits Metdadaten verarbeitbare Informationen über Gruppierungen, Organisationen und Individuen bieten.[41] Mit diesen Alternativmöglichkeiten und dem Ziel einer egalitären Kryptographie ist das CSS sowohl aus konsequentialistischer als auch aus menschenrechtlicher Perspektive abzulehnen.[42] Weder in der Form einer EU-Chatkontrolle noch im allgemeinen Sinne sollte das CSS breitflächig umgesetzt werden.[43] Die Kryptographinnen und Kryptographen Abelson u. a. bezeichnen das CSS dann auch als das, was es im Eigentlichen ist – ein automatisiertes Werkzeug der Massenüberwachung:

> In reality, CSS is bulk intercept, albeit automated and distributed. As CSS gives government agencies access to private content, it must be treated like wiretapping. In jurisdictions where bulk intercept is prohibited, bulk CSS must be prohibited as well. […] Introducing this powerful scanning technology on all user devices without fully understanding its vulnerabilities and thinking through the technical and policy consequences would be an extremely dangerous societal experiment.[44]

In der Europäischen Union fand sich bis einschließlich 2024 keine Mehrheit im Rat, womit das verpflichtende CSS zumindest vorerst und im Rahmen der Legislatur 2019–2024 gescheitert war.[45] Überraschend war in diesem Prozess jedoch lange Zeit, welch breite Unterstützung das Vorhaben seitens zahlreicher Regierungen der Mitgliedstaaten genossen hatte.[46]

---

41 Ob und unter welchen Umständen die Analyse von Metdadaten ethisch erlaubt oder gar geboten sein sollte, kann an dieser Stelle nicht abschließend diskutiert werden. Metadaten und die Ethik der Kryptographie noch stärker in Zusammenhang zu bringen, wird Aufgabe späterer Arbeiten sein.

42 Alternative Möglichkeiten werden etwa genannt bei ebd., S. 12.

43 Noch deutlicher formuliert hier Kelber eine Kritik am CSS im Kontext der vorgeschlagenen EU-Verordnung: „Zur Bekämpfung des sexuellen Kindesmissbrauchs sollten effektive und zielgerichtete Maßnahmen umgesetzt werden. Eine anlasslose und unverhältnismäßige Massenüberwachung gehört nicht dazu. So etwas kennen wir ansonsten nur aus autoritären Staaten. Einmal eingeführt, droht auch in Europa eine Ausweitung der überwachten Inhalte. Das zeigen die Erfahrungen der Einführung anderer Überwachungsmaßnahmen"; ebd., S. 3.

44 Abelson u. a., *Bugs in our Pockets*, S. 2.

45 Siehe Andre Meister. „Verpflichtende Chatkontrolle vorerst gescheitert". In: *Netzpolitik.org* (13. Dez. 2023). URL: https://netzpolitik.org/2023/etappensieg-verpflichtende-chatkontrolle-vorerst-gescheitert/ (besucht am 15.04.2024).

46 Siehe Andre Meister. „Immer mehr EU-Staaten gegen unverhältnismäßige Chatkontrolle". In: *Netzpolitik.org* (23. Nov. 2023). URL: https://netzpolitik.org/2023/internes-protokoll-immer-mehr-eu-staaten-gegen-unverhaeltnismaessige-chatkontrolle/ (besucht am 15.04.2024).

Besonders fragwürdig wurde die Unterstützung, nachdem auf politischer Ebene begründete Lobbyismusvorwürfe laut geworden waren, die die EU-Innenkommissarin Ylva Johansson sowie den US-amerikanischen Schauspieler Ashton Kutcher und seine Organisation *Thorn* betrafen.[47] Hinzu kamen nachgewiesene Falschaussagen Johanssons in der deutschen Zeitschrift *Der Spiegel* sowie Vorwürfe eines politisch gesteuerten *Microtargetings*, das explizit in Mitgliedstaaten mit bislang ablehnender Haltung eingesetzt worden war.[48] Eine politische Analyse dieser Vorwürfe ist zwar nicht Teil der vorliegenden Arbeit, der es um die ethischen Aspekte der Technologie geht, sie sollte aber in folgenden Forschungen transparent aufgearbeitet werden. Auch die Abgeordneten des EU-Parlaments sind zu einer kritischeren Kontrolle der Kommission und der Mitgliedstaaten aufgefordert. Für die hier diskutierte Ethik der Kryptographie aber ist in jedem Fall eindeutig, dass das CSS in dieser Form abzulehnen ist.

47 Siehe Manuel G. Pascual. „Fighting pedophilia at the expense of our privacy: The EU rule that could break the internet". In: *El País* (17. Okt. 2023). URL: https://english.elpais.com/technology/2023-10-17/fighting-pedophilia-at-the-expense-of-our-privacy-the-eu-rule-that-could-break-the-internet.html (besucht am 15.04.2024); sowie Alexander Fanta. „How a Hollywood star lobbies the EU for more surveillance". In: *Netzpolitik.org* (12. Mai 2022). URL: https://netzpolitik.org/2022/dude-wheres-my-privacy-how-a-hollywood-star-lobbies-the-eu-for-more-surveillance (besucht am 15.04.2024).

48 *Netzpolitik.org* hat in dem genannten Interview drei Falschaussagen sowie mindestens sieben irreführende Aussagen identifiziert; siehe Sebastian Meineck, Anna Biselli und Markus Reuter. „So führt EU-Kommissarin Ylva Johansson die Öffentlichkeit in die Irre". In: *Netzpolitik.org* (10. Feb. 2023). URL: https://netzpolitik.org/2023/chatkontrolle-so-fuehrt-eu-kommissarin-ylva-johansson-die-oeffentlichkeit-in-die-irre/#netzpolitik-pw (besucht am 15.04.2024). Siehe das Interview in Ralf Neukirch und Wolf Wiedmann-Schmidt. „‚Es geht um viele Kinder, die wir retten können'". In: *Der Spiegel* (10. Feb. 2023). URL: https://www.spiegel.de/politik/deutschland/eu-kommissarin-ylva-johansson-ueber-missbrauch-im-netz-es-geht-um-viele-kinder-die-wir-retten-koennen-a-63bdbf05-f201-4d03-abfd-fd12a83a2d62 (besucht am 15.04.2024). Zum Vorwurf des Microtargetings siehe Markus Reuter. „EU-Kommission schaltet irreführende Werbung für Chatkontrolle auf X". In: *Netzpolitik.org* (13. Okt. 2023). URL: https://netzpolitik.org/2023/politisches-mikrotargeting-eu-kommission-schaltet-irrefuehrende-werbung-fuer-chatkontrolle-auf-x (besucht am 15.04.2024).

8.2 Regulierung über Intermediäre

Im Kontext des CSS hat der vorherige Abschnitt zum einen die Grundannahme (I) widerlegt, dass ein Zugriff auf Klartexte überhaupt nicht mehr möglich sei. Zum anderen ist gezeigt worden, dass überzeugende Argumente gegen eine normative Aussage (II) sprechen, nach der in Situationen mit *sehr guten* Gründen eine Entschlüsselung per Fernzugriff über das CSS möglich sein sollte. Die prozedurale Umsetzung einer solchen Regulierung soll nun vertiefter untersucht werden. Sie betrifft neben dem CSS auch weitere Möglichkeiten zur Regulierung wie etwa Backdoors.

Mit *prozeduraler Umsetzung* ist gemeint, auf welche Art und Weise und mithilfe welcher Institutionen, Intermediäre und Sanktionen eine Regulierung von Kryptographie funktionieren kann. All das ist für eine Ethik der Kryptographie höchst relevant, wurde jedoch in der ethischen Forschung bislang zu wenig rezipiert. Eine Ethik der Kryptographie soll und kann weder eine reine Ethik *der vertraulichen Kommunikation* noch eine reine Ethik *über Privacy* sein. Sie inkludiert vielmehr auch die technologischen und gesellschaftlich-politischen Rahmenbedingungen, die einen entscheidenden Einfluss darauf haben, welche normativen Maßstäbe an eine praktisch anwendbare Kryptographie anzulegen sind.

In Abschnitt 4.3 wurde beschrieben, wie eine Regulierung von Kryptographie möglich ist – entgegen der Vorstellung von Cypherpunks und der Crypto-Anarchie. Mit *Code: Version 2.0* von Lessig sowie *Who Controls the Internet?* von Goldsmith und Wu wurden dabei vier Bereiche möglicher Regulierung von Kryptographie erarbeitet: Beeinflussung der Forschung, Exportbeschränkungen, Backdoors sowie das CSS. Was diesen Möglichkeiten gemein ist, ist eine prozedurale Umsetzung der Regulierung über *Intermediäre*. Abzugrenzen davon ist eine *direkte* Regulierung des Individuums. Letztere könnte beispielsweise per Gesetz die Nutzung von verschlüsselter Kommunikation unter Strafe stellen. Zwar ist dies zumindest für liberal-demokratische Länder offensichtlich problematisch, doch wird der prozedurale Vergleich von direkter und indirekter Regulierung für eine ethische Gesamtbewertung hilfreich werden. Zusammenfassend soll gezeigt werden, dass neben der Grundannahme (I) sowie der normativen Aussage (II) auch die prozedurale Umsetzung (III) einer hier vorgestellten Ethik der Kryptographie widerspricht.

Betrachten wir dazu das Verhältnis von direkter und indirekter Regulierung aus normativer Perspektive. Zunächst ließe sich intuitiv annehmen, dass eine *direkte* Regulierung des Individuums ethisch problema-

tischer sei als eine Regulierung per Intermediäre. Eine direkte Regulierung würde zweifelsfrei einem Grund- und Menschenrecht auf vertrauliche Kommunikation, Privacy und Meinungsfreiheit widersprechen.[49] Es scheint daher auch wenig erfolgversprechend, dass eine direkte Regulierung des Individuums in einem demokratischen Prozess akzeptiert werden würde. Bedeutet das nun aber, dass eine Regulierung über Intermediäre weniger kritisch zu betrachten ist oder es sich zumindest um das *geringere Übel* mit *weniger Kollateralschäden* handelt?

Bei einer Bejahung dieser Fragen ist aus verschiedenen Gründen Skepsis geboten. Letztlich ist, wie im Folgenden analysiert wird, eine Regulierung der Kryptographie über Intermediäre ethisch mindestens ebenso kritisch zu sehen wie eine direkte Regulierung. Zur Begründung werden Argumente diskutiert, die gegen eine ethische Präferenz einer Regulierung über Intermediäre sprechen. Diese Argumente sind nicht nur auf das CSS anwendbar, sondern auf alle Versuche, eine frei zugängliche Kryptographie über Intermediäre zu verhindern, zu reduzieren oder zu beschränken.

Um die folgenden Argumente spezifisch auf den Fall der Kryptographie anwenden zu können, lässt sich auf Lessigs Analysen zurückgreifen. Aus der Perspektive des *code writings* bewertet auch er eine indirekte Regulierung aus normativer Perspektive. Dabei erkennt er zunächst, dass Regierungen regulatorische Ziele erreichen können, ohne politische Konsequenzen befürchten zu müssen:

> Indirectly, by regulating code writing, the government can achieve regulatory ends, often without suffering the political consequences that the same ends, pursued directly, would yield.
>
> We should worry about this. We should worry about a regime that makes invisible regulation easier; we should worry about a regime that makes it easier to regulate. We should worry about the first because invisibility makes it hard to resist bad regulation; we should worry about the second because we don't yet […] have a sense of the values put at risk by the increasing scope of efficient regulation.[50]

Das erste Argument bezieht sich auf die Folgen einer Regulierung über Intermediäre, mit der eine Reduktion der Transparenz verbunden ist. Les-

49 Siehe auch Lessig, *Code*, S. 67. Lessig impliziert hier, dass das Verbot der Nutzung von Kryptographie direkt in die Rechte von Individuen eingreift.

50 Ebd., S. 136–137.

sig erkennt dabei zu Recht: „If transparency is a value in constitutional government, indirection is its enemy. It confuses responsibility and hence confuses politics."[51] Es geht dabei darum, dass die direkte Verbindung von Regulierung und Konsequenz weniger deutlich wird.[52] Ein Beispiel wäre die gewünschte Reduktion von Alkoholkonsum: Bei einer direkten Beschränkung der verkaufbaren Höchstmenge an Personen wäre jeder Person stets bewusst, dass das Ziel des Gesetzgebers eine Reduktion des Konsums ist. Bei einer indirekten und komplexen Steuerung des Alkoholkonsums über eine Anhebung der Alkoholsteuer, die durch die Firmen auf den Preis aufgeschlagen wird, ist das nicht der Fall. Die Käuferin und der Käufer werden nicht sofort, direkt und transparent wissen, warum der Preis erhöht wurde, schließlich könnte es sich beispielsweise auch um eine inflationsbedingte Anpassung handeln.

Für die Kryptographie ist dies in ähnlicher Weise gegeben. Ein direktes Verbot lässt den Einzelnen oder die Einzelne erkennen, dass die eigenen Grundrechte beschnitten werden. Diese Erkenntnis führt gegebenenfalls zur Ablehnung des Verbots, was in einem demokratischen Prozess zur Veränderung beitragen kann. Bei einer Regulierung über Intermediäre jedoch ist schwerer, zu einer solchen Erkenntnis zu gelangen. Wenn Anbieter von Kommunikationsdienstleistungen verpflichtet werden, eine Backdoor zu implementieren oder das CSS umzusetzen, wird die einzelne Person das zunächst kaum wahrnehmen können.

Neben dieser Intransparenz kommt ein Gefühl der Ohnmacht hinzu, da es sich um eine Regulierung der Unternehmen und nicht unmittelbar des Individuums handelt. In beiden Fällen ist eine Veränderung des Verhaltens des Individuums das Ziel des Regulierungsversuchs. Die Möglichkeit, an einem *transparenten* Meinungsbildungsprozesses teilzuhaben, ist im Fall indirekter Regulierung jedoch geringer. Es lässt sich daher auch auf die Kryptographie übertragen, wenn Lessig feststellt:

> The key criticism that I've identified so far is transparency. Code-based regulation – especially of people who are not themselves technically expert – risks making regulation invisible. Controls are imposed for particular policy reasons, but people experience these controls as nature. And that experience, I suggest, could weaken democratic resolve.[53]

51 ebd., S. 133.
52 Siehe ebd., S. 135.
53 Ebd., S. 138.

Im Kontext der Kryptographie widerspricht diese „invisible regulation“[54] in der Konsequenz der Idee einer *egalitären Kryptographie*. Nur Personen, die technisch versiert sind, können diese Regulierung erkennen und umgehen. Die anderen werden keine Maßnahmen zur verschlüsselten Kommunikation ergreifen – mit der Folge, dass einige wenige weiterhin kryptographisch und privat kommunizieren können, der Großteil der Bevölkerung jedoch nicht. Das aber ist das Gegenteil einer egalitären Kryptographie.

Bei indirekter Regulierung von Kryptographie wird jedoch nicht nur verschleiert, dass *überhaupt* eine Regulierung und Steuerung stattfindet, kaschiert ist auch, *wer* dafür verantwortlich ist. So kann die Steuerung der Intermediäre etwa im nicht-öffentlichen Raum stattfinden, beispielsweise im Rahmen von Lobbyismus oder mündlichen Absprachen. Dieses enge Zusammenwirken von Industrie und Politik wird bei einer Regulierung über Intermediäre nur schwer öffentlich und von der Zivilgesellschaft kontrolliert werden können. Bezogen auf solche informellen Absprachen erkennen auch Schulz und van Hoboken Risiken für die Menschenrechte im Bereich der Verschlüsselung:

> Especially informal agreements between government and industry actors can trigger risks for human rights in the area of encryption, since this negatively affects the attribution of acts to governments, which is a precondition to apply human rights most effectively[.][55]

Eine Folge der Intransparenz bei einer solchen Regulierung ist damit die verminderte „attribution of acts to governments“[56] – also eine deutlich geschwächte Zurechenbarkeit von Verantwortung. Zurechenbarkeit ist jedoch eine Eigenschaft, die für demokratische Entscheidungsprozesse und Meinungsbildung eine essentielle Voraussetzung bildet. Im Fall direkter Regulierung des Individuums ist eine Zurechenbarkeit der Verantwortlichkeit gegeben: Wenn für die Bevölkerung ersichtlich ist, *wer* (oder welche Institution, Partei oder Regierung) eine solche direkte Regulierung angeordnet hat oder anordnen will, dann kann die einzelne Person ihre Entscheidung bei der nächsten Abstimmung oder Wahl entsprechend anpassen. Bei einer indirekten Regulierung über Intermediäre ist hingegen

54 Lessig, *Code*, S. 136.
55 Schulz und Hoboken, *Human rights and encryption*, S. 61.
56 Ebd., S. 61.

ohne spezifisches Wissen oft nicht erkennbar, wer für die Regulierung die Verantwortung trägt.

Bei der Regulierung von Kryptographie wäre bei einem direkten Verbot oder einer direkten Beschränkung also stets ersichtlich, dass die Legislative dies so bestimmt hat und die Exekutive es entsprechend durchsetzt. Rechenschaft ablegen müssen hier die regulatorischen Institutionen. Bei einer Regulierung über Intermediäre verhüllt hingegen die Komplexität der Steuerung eine solche Rechenschaftsbeziehung und Verantwortung. Wenn beispielsweise das CSS implementiert wird, trägt aus Sicht der Bevölkerung zunächst das Unternehmen die Verantwortung für die Beschränkung der E2E-Verschlüsselung. Dass aber ursächlich eine regulatorische Pflicht dahintersteht und die Verantwortung und Rechenschaft *nicht* beim Unternehmen liegt, ist nur bei einer vertieften Auseinandersetzung mit der Thematik erkennbar.

Weiter ist für die Betrachtung indirekter und intermediärer Regulierung zu fragen, ob und wie viel Gestaltungsspielraum Intermediäre dabei erhalten sollten. Ein breiter Rahmen, in dem die konkrete Umsetzung den Unternehmen und Organisationen überlassen wird, scheint zunächst nahezuliegen. Damit könnten marktwirtschaftliche Mechanismen zur Verbesserung der Technologie und zur eigentlichen Zielerreichung greifen. Gleichzeitig bedeutet dies aber auch eine Kompetenzübertragung der Legislative respektive Exekutive auf profitorientierte Organisationen. Beim CSS würde sich beispielsweise die Frage stellen, ob die Kriterien zur Analyse der Nachrichten von Unternehmen festgesetzt werden dürfen. Eine solche Kompetenzübertragung von einem demokratischen Entscheidungsort hin zur Wirtschaft wäre wegen mangelnder Kontrollierbarkeit kritisierbar.[57]

Ein eng abgesteckter Gestaltungsspielraum würde dieses Problem zwar umgehen. Gleichzeitig wären jedoch marktwirtschaftliche Lösungen schwerer zu erreichen, und es entstünde ein hoher Verwaltungsaufwand für die Legislative oder die Exekutive. Entschiede die Exekutive über die konkrete Umsetzung der Regulierung, würden sich Fragen nach dem Verhältnis der unterschiedlichen Gewalten und einer gegenseitigen Kontrolle stellen. Dies wäre zum Beispiel dann der Fall, wenn nur eine generelle Implementierung des CSS vom Gesetzgeber vorgegeben wird, die Entschei-

57 Im Kontext von Zensur weist Ross Anderson auf ähnliche Problematiken hin; siehe Anderson, *Security Engineering*, S. 945.

dung über die Kriterien der Analyse und Detektion jedoch der Exekutiven überlassen ist. Auch hier wäre ein Missbrauch des CSS, auf den bereits hingewiesen wurde, durchaus möglich oder sogar wahrscheinlich.[58]

Zusammenfassend wird aus den genannten Gründen deutlich, dass eine Regulierung der Kryptographie über Intermediäre – ob nun mittels CSS, Backdoors oder anderer Maßnahmen – in ethisch-normativer Sicht einer direkten Regulierung keineswegs vorzuziehen ist. Daraus kann indes nicht abgeleitet werden, dass ganz allgemein *gar keine* Regulierung über Intermediäre erfolgen sollte. Andere Bereiche außerhalb der Kryptographie können sicherlich von einer indirekten Regulierung profitieren, beispielsweise im Bereich der Pharmazie. Eine direkte Regulierung des Individuums wäre im medizinischen Bereich komplex, wenig zielführend und kaum effektiv. Stattdessen bietet es sich an, die Hersteller von pharmazeutischen Produkten zu Sicherheit und Effektivität ihrer Erzeugnisse zu verpflichten.[59]

Eine entscheidende Differenzierung ist jedoch dann zu treffen, wenn eine indirekte Regulierung eine *mögliche* Einschränkung von konkreten Grund- und Menschenrechten mit sich bringt. Im Fall der Regulierung pharmazeutischer Hersteller ist kaum von einer solchen auszugehen, wenn das Ziel der Regulierung mehr Sicherheit der medizinischen Produkte ist. Für die Kryptographie ist in den vorherigen Kapiteln jedoch gezeigt worden, dass eine Regulierung hier konkrete Grund- und Menschenrechte betrifft. Die Hürden für eine intransparente Regulierung über Intermediäre sollte in Situationen einer möglichen Einschränkung von Rechten aufgrund der Universalität der Menschenrechte sowie der Fragilität ihrer praktischen Realisierung weit höher angesetzt werden als in Situationen, in denen eine solche Einschränkung der Grund- und Menschenrechte nicht zu erwarten ist. Es kann daher folgendes normatives Prinzip formuliert werden, das auch für die Regulierung der Kryptographie gelten muss:

> *Besteht die Möglichkeit einer Einschränkung der Grund- und Menschenrechte, ist eine indirekte Regulierung ethisch höchstens genauso gerechtfertigt und legitim wie eine (hypothetische) direkte Regulierung.*

58 Siehe zu weiteren Argumenten Abschnitt 8.1.

59 Auch für Lessig bedeutet das nicht, dass Regulierung immer schlecht wäre. Für ihn geht es vielmehr um die genannte Transparenz: „The state has no right to hide its agenda"; Lessig, *Code*, S. 135.

Umgekehrt bedeutet dies, dass eine indirekte Regulierung ethisch nicht positiver bewertet werden kann als eine (hypothetische) direkte Regulierung. Begründet wird dieses Prinzip dadurch, dass der direkte oder indirekte Charakter einer Regulierung keinen Einfluss auf die ethische Bewertung haben sollte, wenn Grund- und Menschenrechte direkt oder in der Konsequenz betroffen sein können. Das Kriterium einer möglichen Einschränkung von Grund- und Menschenrechten ist hier entscheidend. Ist es nicht erfüllt, kann eine indirekte Regulierung etwa durch eine Kosten-Nutzen-Analyse sinnvoller und ethisch legitimer sein als eine direkte Regulierung. Da im genannten Beispiel der Regulierung von Pharmazieunternehmen keine Grund- und Menschenrechte gefährdet sind, gleichzeitig aber durch höhere Sicherheit der Medikamente Menschenleben gerettet werden können, ist eine indirekte Regulierung geeignet. Eine direkte Regulierung, bei der Individuen die Einnahme von unsicheren Medikamenten verboten wird, wäre wenig zielführend. Anders ist es, wenn Grund- und Menschenrechte *durch die indirekte Regulierung selbst* gefährdet sind. In diesem Fall ist eine Kosten-Nutzen-Abwägung irreführend, sie verschleiert die Ziele der Regulierung und reduziert die Möglichkeit demokratischer Partizipation. Das oben formulierte Prinzip ist die Antwort auf diese Problematik. Es kann zur Verdeutlichung in eine konkrete Handlungsempfehlung umgewandelt werden, die dann wie folgt lautet:

> *Sobald durch eine indirekte Regulierung eine Einschränkung der Grund- und Menschenrechte möglich ist, stelle man folgende Frage: Wie wäre eine Regulierung ethisch zu bewerten, wenn es sich statt einer indirekten Regulierung um eine direkte Regulierung des Individuums handeln würde? Die indirekte Regulierung kann nicht positiver bewertet werden als die Antwort auf diese Frage.*

Sowohl das Prinzip als auch die Handlungsempfehlung ist nun auf die Kryptographie anzuwenden, insofern in der Konsequenz eine Einschränkung der Grund- und Menschenrechte durch eine indirekte Regulierung möglich ist. Dass es sich so verhält, hat der bisherige Teil III darlegen können. Wenn wir nach obigem Prinzip handeln, müssen wir die Frage stellen: Wie wäre eine Regulierung ethisch zu bewerten, wenn es sich statt einer indirekten Regulierung der Kryptographie vielmehr um eine direkte Regulierung des Individuums handeln würde? Die Antwort darauf ist, dass eine solche direkte Regulierung ethisch abzulehnen wäre, da mit ihr eine offensichtliche Einschränkung der Grund- und Menschenrechte vorläge. Nach obigem Prinzip, nach dem auch die indirekte Regulierung

höchstens so positiv bewertet werden kann wie eine (hypothetische) direkte Regulierung, muss eine indirekte Regulierung der Kryptographie daher abgelehnt werden.[60]

Resümierend sollte damit auch das CSS daran gemessen werden, wie eine direkte Regulierung von verschlüsselter Kommunikation aussehen würde. Mit ihr würden nicht mehr die Kommunikationsdienstleister bestraft, wenn sie kein CSS implementieren, sondern vielmehr einzelne Personen, wenn sie eine Technologie nutzen, die kein CSS anbietet. Es scheint jedoch zu Recht illegitim, wenn eine Einzelperson eine Geld- oder gar Gefängnisstrafe zu erwarten hätte, weil sie eine vollständige E2E-Verschlüsselung nutzt. Nach dem hier herausgestellten Prinzip gilt, dass eine indirekte Regulierung aufgrund ihrer Auswirkung auf die Grund- und Menschenrechte ethisch nicht eher als legitim gelten kann als eine direkte Regulierung. Auch die Analyse der prozeduralen Umsetzung (III) spricht damit gegen das CSS und jede weitere Beschränkung frei zugänglicher Kryptographie über Intermediäre.

8.3 Zukunft (einer Ethik) der Kryptographie

Bei all den bisherigen Analysen scheint es, als wäre die mathematische Grundlage der Kryptographie bereits abgeschlossen. Wie frei, zugänglich und nutzbar die Kryptographie auch für die Einzelne oder den Einzelnen wird, ist dann nur noch eine Frage der sozial-gesellschaftlichen Förderung. David Kahn stellte bereits in der zweiten Ausgabe von *The Codebreakers* fest, dass den Kampf um Kryptographie und Kryptoanalyse letztlich die Kryptographinnen und Kryptographen gewonnen hätten: „Does this mean that the story of secret writing has ended? In the long term, yes."[61]

In Abschnitt 2.5 ist diese Einschätzung aus technologischer Sicht kritisch beleuchtet worden. Kryptographie ist heute mehr denn je Teil des scheinbar nie endenden Kampfes von *code making* und *code breaking*. Vor

60 Damit wird deutlich, warum Lessigs Vergleich kryptographischer Regulierung mit der Regulierung von Autos nicht passend ist; siehe Lessig, *Code*, S. 67. Die Regulierung von Autos betrifft an keiner Stelle die Grund- und Menschenrechte – weder bei einer indirekten noch bei einer direkten Regulierung. Im Falle der Kryptographie ist dies anders.

61 Kahn, *The Codebreakers*, S. 984.

allem der Algorithmus von Shor hat gezeigt, dass auch der DH-Schlüsselaustausch und RSA angreifbar sind, insofern beide Verfahren auf *unbewiesenen* mathematischen Phänomenen basieren. Aber auch der Sicherheit von AES und anderen Blockchiffren liegt die Annahme zugrunde, dass kein Verfahren oder kein Rechner existiert, der diese Algorithmen effizient brechen könnte.

Diese Erkenntnis bedeutet auch: Eine Ethik der Kryptographie darf sich inhaltlich nicht auf die bisherigen Möglichkeiten der Kryptographie beschränken. Nachdem die letzten Kapitel gezeigt haben, wie *essentiell* vertrauliche und sichere Kommunikation aus konsequentialistischer, anthropologischer und gesellschaftlicher Sicht ist, gerät der Prozess des Entwickelns neuartiger Kryptographie in den Mittelpunkt der ethischen Diskussion. Auch hier sind nämlich die Schutzziele der Informationssicherheit zu unterscheiden. Kahns *The Codebreakers* ist aus der Perspektive der *Vertraulichkeit* geschrieben. Moderne Kryptographie ist aber weit mehr als das. *Hashalgorithmen*, welche die Integrität einer Nachricht bewahren sollen, werden weiterentwickelt.[62] An neuen Methoden zur Authentizität, beispielsweise *Zero-Knowledge Proofs*, wird intensiv geforscht.[63] Und *Homomorphic Cryptography* könnte neue Ansätze schaffen, Privacy und Datenanalyse näher zusammenzubringen.[64] Viele dieser Fragen hat diese Grundlagenarbeit nicht einmal im Ansatz ausdiskutieren können.

Eine Frage über die Zukunft (der Ethik) der Kryptographie soll aber zuletzt herausgegriffen werden: das Verhältnis von Quantum Computing, Verschlüsselung und Ethik. Die Einführung in Abschnitt 2.5 ist hierfür um eine ethische Komponente zu erweitern, die sich auf zwei Bereiche an der Schnittstelle von Quantum Computing und Kryptographie bezieht: einerseits auf die *Post-Quanten-Kryptographie* (engl. *Post-Quantum Cryptography*, abgekürzt PQC), die als Antwort auf den Shor-Algorithmus und

62 SHA-3, der aktuelle Hashing-Standard, ist beispielsweise erst 2015 durch die NIST standardisiert worden; siehe National Institute of Standards and Technology. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. (FIPS PUB 202). Gaithersburg, Aug. 2015. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf (besucht am 15.04.2024).

63 Siehe einführend etwa Menezes, Oorschot und Vanstone, *Handbook of Applied Cryptography*, S. 405–417.

64 Siehe einführend etwa Ciara Moore u. a. „Practical homomorphic encryption: A survey". In: *IEEE International Symposium on Circuits and Systems (ISCAS)*. 2014, S. 2792–2795; oder auch Monique Ogburn, Claude Turner und Pushkar Dahal. „Homomorphic Encryption". In: *Procedia Computer Science* 20 (2013), S. 502–509.

die aktuell eingesetzten asymmetrischen Verfahren gedacht ist,[65] andererseits auf den *Quantenschlüsselaustausch* (engl. *Quantum Key Distribution*, abgekürzt QKD), der eine neuartige Sicherheit auf der Basis einer Quantenkommunikation bieten soll.[66]

Konzeptuell sind beide Bereiche für eine Ethik der Kryptographie fundamental voneinander verschieden. Zugleich besteht in beiden Fällen eine immanente *Unsicherheit*, ob, wann und wie das Quantum Computing respektive eine Quantenkommunikation in der praktischen und alltäglichen Realität nutzbar werden könnte. Einerseits schafft diese Unsicherheit Skepsis gegenüber der Technologie. Andererseits gestattet die Ergebnisoffenheit einigen Optimismus. Vereinfacht formuliert wäre eine Verwirklichung praktikabler und skalierbarer Quantenkommunikation aus der Perspektive der Quantenkryptographie tatsächlich technologisch vorteilhaft, insofern damit ein Quantenschlüsselaustausch möglich wäre. Aus der Perspektive der heutigen asymmetrischen Kryptographie wäre allerdings die Realisierung größerer Quantenrechner verheerend, da dann der allergrößte Teil der heute verschlüsselten Kommunikation entschlüsselbar wäre. Der Mathematiker Michele Mosca bringt dies auf den Punkt, indem er schreibt:

> Harnessing the power of quantum mechanics in large-scale quantum computers will allow us to solve many valuable problems for humanity, but we must first take the catastrophic impact of breaking cybersecurity off the table by developing and deploying a suite a quantum-safe cryptographic tools before quantum computers arrive.[67]

Angesichts der Bedeutung der asymmetrischen Kryptographie für die Gesellschaft und deren Sicherheit ist eine Welt wenig wünschenswert, in der diese Art der Kommunikation nicht mehr möglich ist – eine Welt, in der Finanzdaten veröffentlicht werden, Gesundheitsdaten nur noch mit komplexen Methoden vertraulich sind oder die Authentizität der Kommunikation gefährdet ist. Ein solches Worst-Case-Szenario ist jedoch wenig wahrscheinlich. Der Grund dafür liegt, wie bereits angedeutet, insbeson-

65 Siehe zur Einführung z. B. Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 208–210.

66 Siehe zu einer zugänglichen und nicht-technischen Einführung insbesondere Clarke und Knake, *The Fith Domain*, S. 253–264.

67 Mosca, „Cybersecurity in an Era with Quantum Computers", S. 41.

dere in der Post-Quanten-Kryptographie. Dabei geht es um kryptographische Algorithmen, die gegen böswillige Parteien mit größeren Quantenrechnern resistent sind, gleichzeitig aber keinen solchen Quantenrechner erfordern, sondern auf klassischen Rechnern operieren können. Ähnlich wie bei AES sollte auch die PQC durch das US-amerikanische NIST standardisiert werden. Die dritte Runde des Verfahrens wurde bereits 2022 abgeschlossen: Aus dutzenden Kandidaten wurden schließlich vier Algorithmen ausgewählt.[68]

Damit ist diese Entwicklung und die Implementierung der PQC aber noch nicht abgeschlossen. Der bekannte Kryptograph Daniel Bernstein nannte bereits 2009 drei Gründe, warum wir über Post-Quanten-Kryptographie nachdenken sollten: (1) Die Effizienz der Verfahren müsse erhöht werden. (2) Das Vertrauen in die Verfahren müsse gesteigert werden. (3) Die Nutzbarkeit der Verfahren müsse verbessert werden.[69] Auch fünfzehn Jahre später bleiben diese Bedingungen trotz der NIST-Standardisierung relevant. Denn jene standardisierten Algorithmen sind in ihrer mathematischen Formulierung komplex und benötigen eine gewisse Dauer, bis sie in der Praxis anwendbar und sicher implementiert werden.

In diesem Kontext wird mit Rückbezug auf eine konsequentialistische Perspektive aus Kapitel 5 und Kapitel 6 die Bedeutung der PQC deutlich. Einerseits wären die Konsequenzen für das einzelne Individuum desaströs, wenn keine oder nur eine sehr komplexe vertrauliche Kommunikation möglich wäre. Genauso wären aber negative Folgen für die gesellschaftliche und öffentliche Sicherheit zu erwarten. Jeder Moment der alltäglichen digitalen Kommunikation ist auf eine funktionierende, effiziente und sichere Kryptographie angewiesen. Negative Folgen wären so auch dann zu erwarten, wenn eine neue PQC ineffizient oder fehleranfällig implementiert werden würde.

---

68 Siehe National Institute of Standards and Technology. *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. 5. Juli 2022. URL: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (besucht am 15.04.2024); sowie Gorjan Alagic u. a. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST IR 8413-upd1. National Institute of Standards und Technology, Juli 2022. URL: https://doi.org/10.6028/NIST.IR.8413-upd1 (besucht am 15.04.2024). Siehe zum Prozess auch Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 208–209.

69 Siehe Bernstein, „Introduction to post-quantum cryptography", S. 11.

Die Ethik der Kryptographie wird sich in Zukunft jedoch weniger mit dystopischen Szenarien des Fehlens *aller* Verschlüsselung auseinandersetzen müssen, sondern vielmehr mit der realistischen Situation der PQC und den ethischen Folgen im Hinblick auf die Transparenz und die Gleichheit der Kryptographie. Die Überprüfung der PQC kann letztlich nur von einem kleinen Kreis aus hochspezialisierten Entwicklerinnen und Entwicklern vorgenommen werden. Die Verfahren des DH-Schlüsselaustauschs und RSA sind mathematisch einfacher zu verstehen und können daher von einem breiteren Personenkreis sowohl in der Theorie als auch in der Implementierung überprüft werden. Bei komplexeren und intransparenteren Verfahren wächst nicht nur die Möglichkeit von unentdeckten Schwachstellen, deren Ausnutzung die genannten Folgen haben dürfte, sondern auch die Möglichkeit von *intentionalen* Schwachstellen oder Backdoors. Der öffentliche Standardisierungsprozess der NIST kann zwar die Wahrscheinlichkeit dieser Gefahren reduzieren, vollständig ausschließen lassen sie sich aber insbesondere in der Implementierung letztlich nicht.

Auch die Diskussionen aus Kapitel 7 können nun auf den Fall einer PQC bezogen werden. Wenn eine freie und zugängliche Kryptographie geboten ist, dann muss sie auch einfach und niederschwellig nutzbar sein. Bei einer nicht nutzbaren Kryptographie – ob aufgrund eines Verbots oder infolge der technologischen Komplexität – würde letztlich nur ein kleiner Teil der Bevölkerung auf vertrauliche und private Kommunikation zurückgreifen können. Zum einen wären dies die Kryptographinnen und Kryptographen selbst, die über entsprechendes Wissen verfügen, zum anderen aber auch wohlhabende und mächtige Personen und Institutionen, die sich eine solche Expertise schlicht kaufen könnten, und schließlich bis zu einem gewissen Grad Kriminelle, die aufgrund ihres Handelns einen Anreiz zum Kompetenzerwerb hätten. Das aber würde einer *egalitären Kryptographie* widersprechen.

Für eine egalitäre Kryptographie, die überall auf der Welt zugänglich ist und tatsächlich auch von allen genutzt wird, ist zudem nicht nur das Vertrauen der Kryptographinnen und Kryptographen in die Algorithmen von Relevanz. Vertrauen braucht es auch seitens des Individuums, denn wenn eine Person kein Vertrauen in die Technologie hat und davon ausgeht, dass diese abhörbar und nicht sicher ist, wird sie sich in der Kommunikation anders verhalten, als wenn sie einen geschützten,

privaten und sicheren Kommunikationsrahmen vermutet.[70] So können etwa später entdeckte Schwachstellen ein solches Vertrauen in die Verschlüsselungstechnologien und die Privatsphäre dezimieren, selbst wenn eine Ausnutzung unwahrscheinlich ist oder nur mit kaum praktizierbaren Angriffstaktiken möglich wäre.

Der letzte ethisch relevante Aspekt in der Diskussion um die PQC ist das Problem der *Vorratsdatenspeicherung* (engl. *data retention*), auf das bereits Abschnitt 2.5 hingewiesen hat.[71] Alle bisherigen Argumente haben sich auf die Echtzeit bezogen – was aber, wenn eine Institution, ein Unternehmen, ein Staat die Kommunikation speichert in der Hoffnung, sie in zehn, zwanzig, dreißig Jahren entschlüsseln zu können? Ethisch relevant ist diese Frage, insofern Daten nicht nur im Hier und Jetzt schützenswert und vertraulich sein sollten. Zuiderveen Borgesius und Steenbruggen erkennen im Kontext der EMRK:

> The above case-law [*Niemietz* case and *Bernh Larsen Holding* case] shows that Article 8 of the ECHR also protects communications after the transport has ended, regardless of the nature of the communication or the technology used.[72]

Sollte das Quantum Computing irgendwann Realität werden, wäre es Drittparteien möglich, einen großen Teil der heutigen Kommunikation zu entschlüsseln. Sollte das erst in einigen hundert Jahren der Fall sein, wären die zu befürchtenden Konsequenzen sicher gering. Falls es aber bereits in wenigen Jahren zu erwarten ist, wären die Folgen schwerwiegender. In unserer Argumentation für eine ubiquitäre, freie und zugängliche Kryptographie müssen wir konsequenterweise auch den zeitlichen Aspekt inkludieren: Die Kryptographie soll nicht nur Vertraulichkeit für heutige Nachrichten ermöglichen, sondern auch für die *vergangene* und die *zukünftige* Kommunikation.

---

70 Dies bezieht sich insbesondere auf den sogenannten *chilling effect*, der bereits in Abschnitt 5.2 diskutiert worden ist.

71 Unabhängig vom Quantum Computing stellen Diffie und Landau im Kontext der Communication Intelligence fest: „A last operational point that bedevils communications intelligence is *retention* – the preservation of intercepted signals for short and long periods of time until they can be processed, cryptanalyzed, interpreted, or used." Diffie und Landau, *Privacy on the Line*, S. 103, allgemein zum Folgenden auch S. 291–294.

72 Zuiderveen Borgesius und Steenbruggen, „The Right to Communications Confidentiality in Europe", S. 319.

Die PQC kann eine solche Gefahr zumindest im Kontext des Quantum Computing verringern, weshalb ihre Entwicklung und Implementierung zu fördern ist. Infolge der Komplexität der Algorithmen und ihrer Implementierung hat jedoch der aktuelle Stand der PQC eine potentiell größere Ungleichheit in der Entwicklung und Nutzung der Kryptographie zur Folge hat, als dies aktuell bei klassischen Verfahren wie etwa RSA der Fall ist. Wie ausgeprägt diese potentielle Gefahr in wenigen Jahren sein wird, hängt maßgeblich von der gesamtgesellschaftlichen Bildung über Kryptographie, von der Ausbildung der Kryptographinnen und Kryptographen an Universitäten oder in Unternehmen und letztlich auch von einer Reflexion über die ethische Relevanz der entwickelten Algorithmen ab.

Dies ist die eine Seite der Zukunft der Kryptographie, der Ethik und des Quantum Computing. Ein anderes Verhältnis von Ethik und Kryptographie lässt sich beim Quantenschlüsselaustausch erkennen.[73] Ein solcher Algorithmus wäre bei einer alltäglichen Realisierung nicht per se disruptiv-zerstörend für vertrauliche und dezentrale Kommunikation. Im Gegenteil, eine QKD verzichtet wie der DH-Schlüsselaustausch auf eine dritte, zentrale Partei. Anders als bei der bisherigen asymmetrischen Verschlüsselung ist etwa das BB84-Protokoll zudem *unconditionally secure*.[74] Dies bedeutet, dass selbst eine angreifende Partei mit unbegrenzter Rechenkapazität keine Chance hätte, den Schlüssel zu berechnen. Zwar ist hier begründete Skepsis angebracht, was Nutzbarkeit und fehlerfreie Implementierung in naher Zukunft betrifft, doch lässt auch das der *Unsicherheit* Spielraum. Dies spricht wiederum für die Notwendigkeit einer Ethik der Kryptographie in der Quantenkommunikation.[75]

Die QKD würde bei einer praktischen Realisierung das bisherige, tendenziell egalitäre Verhältnis von Staat und Individuen, von Unternehmen und Einzelnen neu definieren. Bei digitaler Kryptographie genügt ein generalistischer Personal Computer (PC), um ein hohes Maß an Vertraulichkeit zu gewährleisten. Für die QKD ist hingegen eine hochspe-

73 Ein Beispiel wäre der BB84-Schlüsselaustausch; siehe Bennett und Brassard, „Quantum Cryptography".

74 Siehe Hoi-Kwong Lo und Hoi Fung Chau. „Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances". In: *Science* 283.5410 (1999), S. 2050–2056.

75 Siehe zur Einführung in skeptische Positionen Hoofnagle und Garfinkel, *Law and Policy for the Quantum Age*, S. 290–292.

zialisierte Hardware erforderlich, die zumindest zu Beginn lediglich die mächtigsten Staaten, Organisationen und Unternehmen zu entwickeln und zu erwerben imstande sein dürften. Zumindest eine gewisse Zeit über wäre das einzelne Individuum somit auch weiterhin auf bisherige Kryptographie angewiesen, die nur *computationally secure* ist. Für wenige andere Parteien könnte Kommunikation dagegen sogar *information-theoretic secure* werden – ohne die Gefahr, dass diese Kommunikation selbst in späteren Jahren noch entschlüsselt werden könnte.[76] Auch dies würde der Idee einer egalitären Kryptographie fundamental widersprechen.

Man könnte nun davon ausgehen, dass diese sichere Form der Verschlüsselung nicht für den alltäglichen Gebrauch notwendig sei. Man könnte vielleicht auch sagen, dass solche Technologien sicherlich nach der unternehmerischen und staatlichen Nutzung bald auch für Individuen zugänglich werden würden. Aber selbst unter der Bedingung, dass eine Quantenkommunikation so günstig und nutzbar werden würde wie die digitale Kommunikation: Wie würde sich dies auf die Versuche einer Regulierung der Kryptographie auswirken? Simon Singh erkennt in seinem populär gewordenen Buch über die Geschichte der Kryptographie zu Recht:

> Diese Technik wird den sicheren Nachrichtenverkehr für Staat, Militär, Wirtschaft und Öffentlichkeit gewährleisten. Offen bliebe einzig die Frage, ob der Staat uns erlauben würde, diese Technik zu verwenden. Wie könnte der Gesetzgeber die Quantenkryptographie so regulieren, daß sie das Informationszeitalter bereichert und nicht die Kriminellen schützt?[77]

Genauso wie im Bereich digitaler Kryptographie scheint es jedoch abwegig, dass eine solche Regulierung je existieren könnte und sollte. Zugleich bedeutet aber auch in der Quantenkryptographie der Erfolg der theoretischen Algorithmen nicht, dass staatliche Institutionen machtlos wären. Implementierungsfehler, die Beschlagnahmung von Geräten, Schwachstellen – all diese Faktoren werden durch eine Quantenkryptographie nicht irrelevant. Sie können auch im 21. Jahrhundert (aus-)genutzt werden, um in spezifischen Fällen Informationen aus der kryptographischen, privaten und sicheren Kommunikation zu ermitteln.

76 Siehe einführend ebd., S. 257–264.

77 Singh, *Geheime Botschaften*, S. 421.

Trotzdem ist davon auszugehen, dass eine freie, zugängliche und ubiquitäre Quantenkryptographie vermutlich einen neuen Crypto War anfeuern wird, bei dem Bürgerrechte und Ethik erneut zur Disposition stehen werden. Zu stark dürfte das Narrativ verfangen, dass die Quantenkryptographie so gut werde, dass nun doch die Anarchie drohe. Auch hier werden die einen diese Anarchie begrüßen, die anderen hingegen vor ihr warnen. Es bleibt zu hoffen, dass in diesem neue Crypto War die Argumente der hier vorgestellten Ethik der Kryptographie Gehör finden werden.

Schluss und Ausblick

Warum sollte man über Ethik *und* Kryptographie nachdenken? Was haben zwei so verschieden wirkende Bereiche miteinander zu tun? Warum braucht es eine Ethik der Kryptographie? Beide Professionen haben schließlich ihren eigenen Kontext, ihre eigene Daseinsberechtigung, ihre eigene Wissenschaft. Es war das Ziel der vorangehenden acht Kapitel, nichts von dem Genuinen beider Wissenschaften zu verlieren – und trotzdem den gegenseitigen Anschluss zu finden. Denn gerade wegen ihrer Verschiedenheit haben sich diese Bereiche einiges zu sagen.

Wir sollten ethisch über Kryptographie nachdenken, weil die Kryptographie mit unserem modernen Alltag verflochten ist wie wenige andere Wissenschaften. Im 21. Jahrhundert werden in jedem Moment Bankdaten über das Internet ausgetauscht, unsere E-Mail-Accounts werden auf den Smartphones synchronisiert, wir empfangen und senden Nachrichten auf den unterschiedlichsten Messengerdiensten. In allen Situationen verlassen wir uns darauf, dass die Kommunikation vertraulich, privat und integer ist. Wäre sie das nicht, dann wären auch all diese alltäglichen Technologien nicht mehr sicher und in dieser Weise nutzbar. Die heutige Gesellschaft ist damit auf Kryptographie angewiesen. Und wenn sie auf so etwas Essentielles angewiesen ist, stellt sich zwangsläufig auch die Frage nach dem *richtigen* Umgang mit dieser Technologie.

Wir sollten aber auch deswegen ethisch über Kryptographie nachdenken, weil diese ubiquitäre Kryptographie in der Geschichte der Menschheit einmalig ist. Über Jahrhunderte war die Verschlüsselung von Nachrichten eine Art Geheimwissenschaft, und das einzelne Individuum wusste meist wenig bis nichts davon. Die Kryptographie wurde zur Geheimniskrämerei, zur Diplomatie, zu Intrigen genutzt. In der zweiten Hälfte des 20. Jahrhunderts vollzog sich jedoch ein fundamentaler Paradigmenwechsel: Die ehemals Klassische Kryptographie wurde zur *Modernen Kryptographie*. Claude Shannon hat die Kryptographie als rigorose Mathematik beschrieben. Der *Data Encryption Standard* (DES) wurde zum Politikum der NSA, von Forschenden und der Zivilgesellschaft. Und mit der asymmetrischen Kryptographie wurde etwas erreicht, was lange Zeit für unmöglich gehalten worden war: sichere Kommunikation über unsichere Kanäle. All dies hat dazu geführt, dass Kryptographie

nun Teil der Informationssicherheit ist und – neben Vertraulichkeit – auch Authentizität garantieren kann.

Kryptographie wurde damit nutzbar für *alle*, sowohl für Individuen als auch für Staaten und Unternehmen. Dank rigoroser mathematischer Verfahren konnten die und der Einzelne zum ersten Mal in der Menschheitsgeschichte in hohem Maße vertraulich kommunizieren. Während mächtige Institutionen immer wieder von Neuem versuchten, den Standard der Modernen Kryptographie umzukehren, hielt ein gewisses Maß an egalitärer Kryptographie Einzug in den Alltag der Menschen. Dieser Paradigmenwechsel und diese vollkommene Neubestimmung dessen, *wer* mithilfe von Kryptographie kommunizieren kann, hatte allerdings einschneidende gesellschaftliche Spannungen zur Folge.

Für die einen war und ist die Kryptographie ein Mittel zur Befreiung, zum Liberalismus, zum Schutz vor Unterdrückung. Phil Zimmermanns Software *Pretty Good Privacy* (PGP) war gleichsam die dazu passende Verkörperung der theoretischen Mathematik in der Gesellschaft. Mit dieser Software zur E-Mail-Verschlüsselung konnten Individuen überall auf der Welt auch *faktisch* verschlüsselt kommunizieren. PGP wurde damit zum Prototyp des Cryptoaktivismus, der sich ab den 1990er-Jahren gebildet hatte. Für solche Cryptoaktivistinnen und Cryptoaktivisten ist die Kryptographie Motiv, Mittel und Ziel einer Gesellschaftsutopie. Die extremste Utopie vertraten aber die Cypherpunks. Kryptographie war und ist für sie nicht einfach ein Briefumschlag, mit dem eine einigermaßen vertrauliche Kommunikation möglich sein soll. Für sie sollte Kryptographie viel radikaler sein als das, für sie war es eine neue Art und Weise, wie die Welt von morgen aussehen konnte: libertär, frei, anarchistisch. Die Kryptographie musste entsprechend *unregulierbar* sein.

Trotz der scharfsinnigen, wenn auch teilweise polemischen Argumente der Cypherpunks ist die Hypothese falsch, Kryptographie sei *nur* eine technologische Angelegenheit. Gerade die frühen Cypherpunks vertraten oft einen Determinismus, dem zufolge die Kryptographie zur *unausweichlichen* Veränderung der Gesellschaft beitragen würde. *Unausweichlich* – das bedeutet: keine Alternative, keine Wahl, keine Entscheidung. Wir müssten nur noch akzeptieren, dass die libertäre Zukunft heute schon angekündigt sei. Wer könne schon die Gesetze der Mathematik und der Kryptographie brechen – kein Staat könne dies, kein Unternehmen, niemand.

Demgegenüber hat diese Arbeit zeigen können, dass Kryptographie eben doch nicht unaufhaltsam ist, dass Verschlüsslung kein Determinis-

mus, sondern doch regulierbar ist. Mit dem Verhältnis von Internet und Kryptographie ist vieles aus dem Bereich der Regulierung des Internets auch auf die Nutzung der Kryptographie anwendbar. *Code: Version 2.0* von Lawrence Lessig sowie *Who Controls the Internet?* von Jack Goldsmith und Tim Wu bilden das Modell, mit dem sich eine Regulierung der Anwendung von Kryptographie systematisch einordnen lässt. Die Crypto Wars der letzten Jahrzehnte, in denen teils heftig um den politischen Umgang mit Kryptographie, Exportbeschränkungen und Backdoors gerungen wurde, stehen sinnbildlich für die Möglichkeiten einer Regulierung.

Wie aber *sollen* wir diese systematischen Versuche der Regulierung normativ bewerten? Wie *sollen* wir eigentlich mit Kryptographie umgehen? Die Ethik als Wissenschaft über Moral ist es, die diese Fragen an der Schnittstelle von Technologie und Gesellschaft zu beantworten hat. Dazu gibt es nicht die *eine* ethische Theorie, die nur noch auf die Fragen der Kryptographie anzuwenden wäre. Methodologisch hat diese Arbeit daher einen pragmatischen Ansatz verfolgt, der sich der Unterschiede der ethischen Zugänge bewusst ist, sich aber hütet, nur *eine* Art der normativen Begründung zuzulassen. Zwei der prominentesten Zugänge sind einerseits die Pflichtethik und andererseits der Konsequentialismus. Anhand verschiedener Beispiele im Kontext der Kryptographie sind die verschiedenen Begründungsweisen deutlich geworden. Als weiteren Zugang bietet sich eine menschenrechtsbasierte Perspektive an. Gerade wenn wir von einer globalen und ubiquitären Kryptographie sprechen, ist die Inklusion des Menschenrechts auf Achtung des Privatlebens sowie des Menschenrechts auf freie Meinungsäußerung naheliegend.

Mit diesen unterschiedlichen Zugängen konnte die Schnittstelle von Kryptographie und Ethik ausgeleuchtet werden. Dennoch sind mit Lessigs *latent ambiguities* Spezialfälle denkbar, bei denen Antworten auf ethische Fragen undurchsichtig und doppeldeutig sein können. Auch im Bereich der Kryptographie können wir methodisch nicht immer von bestimmten Normen oder Konstitutionen ausgehen, die uns Antworten auf den korrekten Umgang mit Kryptographie liefern. Indem Normen aus ihrem Kontext gerissen werden, entstehen Anwendungs- und Wertefragen. All dies macht weitere und umfassendere Analysen zu den unterschiedlichen Argumenten im Umgang mit Kryptographie notwendig, bei denen zu fragen ist, welche *Begründungen* und *Intentionen* für oder gegen den Einsatz von Kryptographie sprechen.

So führen konsequentialistische Argumentationen oft zu Situationen, in denen Zielkonflikte abgewogen werden müssen. Im Kontext der

Kryptographie können solche Zielkonflikte auch als Dichotomien bezeichnet werden und sind so oder so ähnlich immer wieder im politisch-gesellschaftlichen Diskurs als Argument *gegen* eine ubiquitäre Kryptographie genannt worden. Die erste Dichotomie ist am naheliegendsten: die *Dual-Use-Kryptographie* – einerseits genutzt zum Guten, andererseits genutzt zum Schlechten. Anhand einer Kritik am generellen Dual-Use-Gedanken und einer utilitaristischen Perspektive auf die Kryptographie ist eine solche Charakterisierung allerdings abzulehnen. Diese Auseinandersetzung hat anschließend auch ergeben, dass keine *Privacy-vs.-Sicherheit*-Dichotomie existiert. Nach dieser würden wir Sicherheit gewinnen können, wenn wir Privatsphäre reduzieren. Die problematischste aller Dichotomien ist aber die, die als *Überwachung vs. Kryptographie* bezeichnet werden kann. Das Argument dabei ist, dass Kryptographie die Überwachung und Strafverfolgung unmöglich mache. Ironischerweise unterscheiden sich die Verfechterinnen und Verfechter dieses Arguments damit von den Cypherpunks nur in der Bewertung: Die einen sehen es als *gut*, die anderen als *schlecht* an. Der Realität entspricht auch diese letzte Dichotomie jedoch nicht, wie mit Blick auf die Analysemöglichkeiten von Metadaten und die Schwächen kryptographischer Implementierungen eruiert worden ist.

Verkürzt wäre es aber, *nur* über Dichotomien und Zielkonflikte der Kryptographie nachzudenken. Drei Leitmotive und Spezialthemen der Modernen Kryptographie erweitern nämlich ein allzu konsequentialistisch geprägtes Bild von Verschlüsselungstechnologien: Transparenz, Gleichheit und Identität. Obwohl Kryptogrographie *im engeren Sinne* das Ziel verfolgen kann, Vertraulichkeit und Geheimhaltung zu wahren, ist ihr Verhältnis zur Transparenz *im weiteren Sinne* komplexer. Algorithmen müssen nach Kerckhoffs' Prinzip einerseits veröffentlicht werden, andererseits erlaubt das Whistleblowing eine Neubestimmung von Transparenz und Privatsphäre. Das Motiv der Gleichheit ermöglicht zudem das Konzept einer *egalitären Kryptographie*. Bei ihr handelt es sich um die Kombination von Moderner Kryptographie und tatsächlicher Nutzung, unabhängig von Stand, Wissen, Kapital oder Herkunft. Nicht nur Kryptographinnen und Kryptographen, sondern auch Journalistinnen und Journalisten, die Politik und die Gesellschaft sind zur Verwirklichung einer solchen egalitären Kryptographie aufgerufen. Das letzte Motiv hat eine dedizierte Auseinandersetzung mit dem Schutzziel der Authentizität notwendig gemacht. Bislang ist die Identifizierung durch kryptographisch garantierte Authentizität ein Aspekt, der in der ethischen Forschung zu

wenig beachtet wird. Dabei ist die Gefahr groß, dass in dieser Verbindung Identifikationsmechanismen unumgänglich und ubiquitär werden, ohne dass dies zuvor gesellschaftlich und ethisch (aus-)diskutiert und verhandelt worden wäre.

Die ethische Analyse der Kryptographie ist aber nicht nur von theoretischer Relevanz. In der Synthese der technologischen, gesellschaftlichen *und* ethischen Perspektiven sind drei Beispiele diskutiert worden, in denen eine Ethik der Kryptographie notwendig ist. Das *Client-Side-Scanning* (CSS), das im deutschsprachigen Raum unter dem Begriff der *Chatkontrolle* bekannt geworden ist, ist die heute prominenteste Ausprägung einer gewollten Beschränkung und Regulierung von vertraulicher Kommunikation. Mit konsequentialistischen, pflichtethischen und menschenrechtsbasierten Argumenten ist jedoch ersichtlich geworden, dass das CSS in dieser Form kritisiert werden muss. Wie beim CSS handelt es sich bei einer Regulierung von Kryptographie in den allermeisten Fällen zudem um eine *indirekte* Regulierung über Intermediäre. Trotz der praktischen Vorteile ist auch diese Art der Regulierung im Kontext der Kryptographie abzulehnen, sobald eine Verletzung von Grund- und Menschenrechten möglich ist. Und trotz dieser Argumente ist vieles im Bereich der Zukunft einer (Ethik der) Kryptographie noch unklar. Eine praktische Realisierung der Post-Quanten-Kryptographie sowie ein möglicher Quantenschlüsselaustausch würden die Ethik neu herausfordern und vor die Frage stellen, ob und wie eine egalitäre Kryptographie auch in den nächsten Jahrzehnten realisierbar sein wird.

Mit diesen Beispielen ist die Auseinandersetzung mit einer Ethik der Kryptographie jedoch noch lange nicht abgeschlossen. Vieles an der Schnittstelle von Technologie, Gesellschaft und Ethik werden zukünftige Arbeiten vertiefter diskutieren oder gar neu definieren müssen. So lassen sich *innerhalb* der Ethik weitere Zugänge erarbeiten. Die vorliegende Untersuchung hat sich insbesondere auf die Deontologie, den Konsequentialismus sowie die Menschenrechte fokussiert. Welche Argumente kann aber beispielsweise ein tugendethischer Zugang zur Ethik der Kryptographie beitragen? Könnte auch eine Diskursethik in diesem spezifischen Kontext von Technologie und Gesellschaft hilfreich sein? Und wie lassen sich all diese Erkenntnisse ganz praktisch in die alltäglichen, medialen und politischen Prozesse integrieren?

Methodologisch haben sich die bisherigen Diskussionen primär mit einer normativen Perspektive auf die Kryptographie beschäftigt. Doch auch eine empirische Untersuchung im Sinne einer deskriptiven Ethik

wäre eine Bereicherung für die Ethik der Kryptographie. Bislang gibt es aus soziologischer, ethnologischer und quantitativer Perspektive kaum umfassende Untersuchungen und Forschungen zu diesem Thema. Doch was denken die Menschen eigentlich über Kryptographie? Denken sie überhaupt darüber nach? Was wissen Individuen in den unterschiedlichsten Kulturen über Verschlüsselungstechnologien und deren Bedeutung für das gesellschaftliche Zusammenleben? Wie sollen wir ihrer Meinung nach mit Kryptographie umgehen?

Darüber hinaus gibt es konzeptuell völlig neue Möglichkeiten, die die Kryptographie thematisch erweitern und bislang zu wenig ethisch diskutiert worden sind. Themen wie Kryptowährungen, Spyware und Staatstrojaner erfordern eine spezifischere Auseinandersetzung, als sie für die Begründung einer Ethik der Kryptographie möglich ist. Was bedeuten etwa *Privacy Coins* für das reklamierte Währungsmonopol des Staates? Was für Folgen haben *digitale Zentralbankwährungen* für das Individuum und die Gesellschaft? Welche normativ-ethischen Probleme treten im Umgang mit Spyware und Staatstrojanern auf? Wie kann die Kryptographie in all diesen Fällen dem Individuum dienen und nicht den autokratischen und illiberalen Regimen der Welt?

Denken lässt sich aber auch an bislang noch utopische Ideen wie die einer *Liquid Democracy*, einer Verbindung von direkter und repräsentativer Demokratie, die eine Möglichkeit zur *freiwilligen* direkten Mitbestimmung bieten könnte. Über das beste politische System wird seit Jahrhunderten gestritten. Mit dem Paradigma der Modernen Kryptographie sind der Kreativität neuer, unbekannter und vor allem radikaler Ideen über das politische Abstimmungssystem von morgen kaum mehr Grenzen gesetzt. Wird mithilfe von Kryptographie mehr Mitbestimmung möglich sein? Lässt sich in Zukunft vielleicht sogar eine demokratischere Partizipation erzielen?

All das sind Fragen, die im Ausblick einer Ethik der Kryptographie behandelt werden sollten. Damit können wir abschließend zu Recht fragen, ob die vielleicht größte Gefahr im Umgang mit Kryptographie nicht so sehr die Absicht ist, sie zu unterdrücken oder zu beschränken. Immerhin scheint eine Welt, in der keine autokratischen Regime existieren werden, die eine egalitäre Kryptographie verhindern wollen, realitätsfern. Die viel größere Gefahr mag daher in der Annahme liegen, dass eine solche Regulierung, Steuerung und vor allem *Entscheidung* über den Umgang mit Kryptographie gar nicht möglich ist. Ein solches Verständnis von Kryptographie als Nihilismus, als Realität, als Status quo verleitet zur

Resignation, zur Beliebigkeit, zur ethischen Belanglosigkeit. Um dem entgegenzuwirken, sollte eine Ethik der Kryptographie sowohl in der Ethik als auch in der Kryptographie Gehör finden. Nicht nur Kryptographinnen und Kryptographen sind aufgerufen, ethisch zu handeln, auch die Ethik selbst muss beginnen, die Kryptographie zu verstehen, um sie schließlich in den Fachdiskurs und die Gesellschaft einbringen zu können.

Letztlich wird sich die Gesellschaft von morgen entscheiden müssen, ob in Zukunft die Kryptographie nur für wenige zugänglich sein soll – oder doch für viele; ob sie das Modell der Klassischen Kryptographie verfolgen will – oder das der egalitären Kryptographie. Wie sich die autokratischen Systeme entscheiden, in denen all jene Regulierungen mit Brutalität durchgesetzt werden, dürfte klar sein. Gleichzeitig wird die Fragilität einer freiheitlich-demokratischen Gesellschaft an wenigen Themen so deutlich wie am Umgang mit Kryptographie. Auch in liberalen Demokratien ist der Wunsch nachvollziehbar, die negativen Folgen von Verschlüsselung zu minimieren. Sind damit aber Grund- und Menschenrechte betroffen, gilt es für diese Gesellschaften vorsichtig zu sein.

Literatur

Abelson, Hal 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).

Abelson, Hal 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).

Abelson, Harold 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.

Adams, Carlisle. *Introduction to Privacy Enhancing Technologies: A Classification-Based Approach to Understanding PETs*. Cham: Springer, 2021.

Adkins, Lauren D. „Biometrics: Weighing Convenience and National Security against Your Privacy". In: *Michigan Telecommunications and Technology Law Review* 13.2 (2007), S. 541–555.

Alagic, Gorjan u. a. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST IR 8413-upd1. National Institute of Standards und Technology, Juli 2022. URL: https://doi.org/10.6028/NIST.IR.8413-upd1 (besucht am 15.04.2024).

Aljifri, Hassan und Diego Sánchez Navarro. „International legal aspects of cryptography". In: *Computers & Security* 22.3 (2003), S. 196–203.

Amarasinghe, Niluka, 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.

Anderson, Patrick D. „Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange". In: *Ethics and Information Technology* 23.3 (2021), S. 295–308.

Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3. Aufl. Indianapolis: Wiley, 2020.

Andress, Jason und Steve Winterfeld. *Cyber Warfare*. 2. Aufl. Waltham: Syngress, 2014.

Arnold, Jason Ross. *Whistleblowers, Leakers, and Their Networks: From Snowden to Samizdat*. Lanham u. a.: Rowman & Littlefield, 2020.

Arslanian, Henri. *The Book of Crypto: The Complete Guide to Understanding Bitcoin, Cryptocurrencies and Digital Assets*. Cham: Palgrave Macmillan, 2022.

Assange, Julian u. a. *Cypherpunks: Freedom and the Future of the Internet*. New York und London: OR Books, 2012.

Assmann, Jan. „Zur Ästhetik des Geheimnisses. Kryptographie als Kalligraphie im alten Ägypten". In: *Zeichen zwischen Klartext und Arabeske. Konferenz des Konstanzer Graduiertenkollegs „Theorie der Literatur". Veranstaltet im Oktober 1992.*

Hrsg. von Susi Kotzinger und Gabriele Rippl. Amsterdam und Atlanta: Rodopi, 1994, S. 175–186.

Ball, Kristie, Kevin D. Haggerty und David Lyon, Hrsg. *Routledge Handbook of Surveillance Studies*. London und New York: Routledge, 2014.

Bambauer, Derek E. „Privacy versus Security". In: *The Journal of Criminal Law and Criminology* 103.3 (2013), S. 667–683.

Bamford, James. „The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)". In: *Wired* (12. März 2015). URL: https://www.wired.com/2012/03/ff-nsadatacenter/ (besucht am 15.04.2024).

– *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*. Harmondsworth: Penguin Books, 1983.

Barendt, Eric. „Balancing Freedom of Expression and Privacy: The Jurisprudence of the Strasbourg Court". In: *Journal of Media Law* 1.1 (2009), S. 49–72.

Barlow, John Perry. *A Declaration of the Independence of Cyberspace*. Davos, 8. Feb. 1996. URL: https://www.eff.org/de/cyberspace-independence (besucht am 15.04.2024).

– *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).

Bartlett, Jamie. *The People Vs Tech: How the internet is killing democracy (and how we save it)*. London: Ebury Press, 2018.

Bauer, Craig P. *Secret History: The Story of Cryptology*. 2. Aufl. Boca Raton, London und New York: CRC Press, 2021.

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

Bellovin, Steven M. „Frank Miller: Inventor of the One-Time Pad". In: *Cryptologia* 35.3 (2011), S. 203–222.

Beltramini, Enrico. „Against technocratic authoritarianism: A short intellectual history of the cypherpunk movement". In: *Internet Histories* 5.2 (2021), S. 101–118.

Bennett, Charles H. und Gilles Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing". In: *Proceedings of the International Conference on Computers, Systems and Signal Processing. Bangalore, India*. 1984, S. 175–179.

Bernal, Paul. „Data gathering, surveillance and human rights: recasting the debate". In: *Journal of Cyber Policy* 1.2 (2016), S. 243–264.

Bernstein, Daniel J. „Introduction to post-quantum cryptography". In: *Post-Quantum Cryptography*. Hrsg. von Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen. Berlin und Heidelberg: Springer, 2009, S. 1–14.

Bernstein, Daniel J., Johannes Buchmann und Erik Dahmen, Hrsg. *Post-Quantum Cryptography*. Berlin und Heidelberg: Springer, 2009.

Bernstein, Daniel J. und Tanja Lange. „Post-quantum cryptography". In: *Nature* 549 (2017), S. 188–194.

Berret, Charles. „The Cultural Contradictions of Cryptography: A History of Secret Codes in Modern America". Dissertation. New York: Columbia University, 2019. URL: https://academiccommons.columbia.edu/doi/10.7916/d8-3h8z-4t93 (besucht am 15.04.2024).

Beutelspacher, Albrecht. *Geheimsprachen und Kryptographie: Geschichte, Techniken, Anwendungen*. 6. Aufl. München: C. H. Beck, 2022.

Biham, Eli und Adi Shamir. „Differential Cryptanalysis of DES-like Cryptosystems". In: *Journal of Cryptology* 4.1 (1991), S. 3–72.

Blaze, Matt. „Protocol Failure in the Escrowed Encryption Standard". In: *Proceedings of the 2nd ACM Conference on Computer and Communications Security. Fairfax, Virginia*. CCS '94. Association for Computing Machinery, 1994, S. 59–67.

Bolotinsky, Avi, Anita Ritscher und Philip Cheung. „Dieser Iraner kämpft im Internet für Freiheit". In: *Neue Zürcher Zeitung* (3. Juni 2023). URL: https://www.nzz.ch/technologie/sina-rabbani-ein-iranischer-freiheitskaempfer-im-internet-ld.1733694 (besucht am 15.04.2024).

Borowski, Mariusz und Marek Leśniewicz. „Modern usage of 'old' one-time pad". In: *2012 Military Communications and Information Systems Conference. Gdansk, Poland*. 2012, S. 1–5.

Borsook, Paulina. *Cyberselfish: A Critical Romp through the Terribly Libertarian Culture of High Tech*. New York: PublicAffairs, 2000.

– „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).

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*. Reading: Perseus Books, 1998.

Böhm, Otto und Doris Katheder. *Grundkurs Menschenrechte: Die 30 Artikel. Kommentare und Anregungen für die politische Bildung*. Bd. 3. Würzburg: Echter Verlag, 2013.

Büchi, Moritz, Noemi Festic und Michael Latzer. „The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda". In: *Big Data & Society* 9.1 (2022), S. 1–14.

Cammaerts, Bart. „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.

Ceva, Emanuela und Michele Bocchiola. *Is Whistleblowing a Duty?*. Cambridge und Medford: Polity Press, 2019.

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

Chin, Josh und Liza Lin. *Surveillance State: Inside China's Quest to Launch a New Era of Social Control*. New York: St. Martin's Press, 2023.

Chow, Jerry, Oliver Dial und Jay Gambetta. „IBM Quantum breaks the 100-qubit processor barrier". In: *IBM Blog* (16. Nov. 2022). URL: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle (besucht am 15.04.2024).

Christensen, Chris. „Review of *The Imitation Game*". In: *Cryptologia* 41.2 (2017), S. 178–181.

Clapham, Andrew. *Human Rights: A Very Short Introduction*. 2. Aufl. Oxford: Oxford University Press, 2015.

Clark, Andrew J. „Foreword". In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Berlin und Heidelberg: Springer, 2016, S. VII–VIII.

Clarke, Richard A. und Robert K. Knake. *The Fith Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York: Penguin Press, 2019.

Coleman, E. Gabriella. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton und Oxford: Princeton University Press, 2013.

Confalonieri, Roberto u. a. „A historical perspective of explainable Artificial Intelligence". In: *WIREs Data Mining and Knowledge Discovery* 11.1 (2021), e1391.

Connolly, Aisling. „Freedom of Encryption". In: *IEEE Security & Privacy* 16.1 (2018), S. 102–103.

Cook, Philip und Conrad Heilmann. „Two Types of Self-Censorship: Public and Private". In: *Political Studies* 61.1 (2013), S. 178–196.

Coppersmith, Don. „The Data Encryption Standard (DES) and its strength against attacks". In: *IBM Journal of Research and Development* 38.3 (1994), S. 243–250.

Cox, Ingemar J. u. a. *Digital Watermarking and Steganography*. Burlington: Morgan Kaufmann, 2008.

Daalen, O. L. van. „The right to encryption: Privacy as preventing unlawful access". In: *Computer Law & Security Review* 49 (2023), Artikel 105804.

Dame-Boyle, Alison. *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).

Deigh, John. *An Introduction to Ethics*. Cambridge: Cambridge University Press, 2010.

Derek, Heater. *A Brief History of Citizenship*. Edinburgh: Edinburgh University Press, 2004.

Desmedt, Yvo. „What is the Future of Cryptography?" In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Berlin und Heidelberg: Springer, 2016, S. 109–122.

Deutsch, David. „Quantum theory, the Church–Turing principle and the universal quantum computer". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985), S. 97–117.

Deutsch, David und Richard Jozsa. „Rapid solution of problems by quantum computation". In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 439.1907 (1992), S. 553–558.

Die Bibel. Einheitsübersetzung der Heiligen Schrift. Gesamtausgabe. Stuttgart: Verlag Katholisches Bibelwerk, 2016.

Diffie, Whitfield. *Preliminary Remarks on the National Bureau of Standars Proposal Standard Encryption Algorithm for Data Protection*. Mai 1975. URL: https://stacks.stanford.edu/file/druid:wg115cn5068/1975%200522%20ltr%20to%20NBS.pdf (besucht am 15.04.2024).

Diffie, Whitfield und Martin E. Hellman. „New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), S. 644–654.
– „Privacy and Authentication: An Introduction to Cryptography". In: *Proceedings of the IEEE* 67.3 (1979), S. 397–427.
Diffie, Whitfield und Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Überarbeitete und erweiterte Version. Cambridge, MA, und London: MIT Press, 2007.
Dignum, Virginia. *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*. Cham: Springer, 2019.
Dooley, John F. *Codes, Ciphers and Spies: Tales of Military Intelligence in World War I*. Cham: Copernicus, 2016.
– *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*. Cham: Springer, 2018.
Dostojewskij, Fjodor. *Aufzeichungen aus dem Kellerloch*. 9. Aufl. Aus dem Russsischen von Swetlana Geier. Frankfurt am Main: Fischer Taschenbuch, 2023.
Dreyfus, Suelette. *The Idiot Savants' Guide to Rubberhose: What is Rubberhose?*. URL: https://archive.ph/20121029045140/http://marutukku.org/current/src/doc/maruguide/t1.html (besucht am 15.04.2024).
Drosnin, Michael. *The Bible Code*. New York: Simon & Schuster, 1997.
Dusseldorp, Marc. „Technikfolgenabschätzung". In: *Handbuch Technikethik*. Hrsg. von Armin Grunwald und Rafaela Hillerbrand. 2. Auflage. Stuttgart: J. B. Metzler, 2021, S. 442–446.
Eckert, Claudia. *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. 10. Auflage. Berlin und Boston: De Gruyter Oldenbourg, 2018.
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).
– *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).
Elmer-Dewitt, Philip. „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).
Encryption Working Group. *Moving the Encryption Policy Conversation Forward*. Carnegie Endowment for International Peace, Sep. 2019. URL: https://carnegieendowment.org/files/EWG__Encryption_Policy.pdf (besucht am 15.04.2024).
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).
European Court of Human Rights. *The Sunday Times v. The United Kingdom*. Application no. 6538/74. 26. Apr. 1979.

European Parliamentary Research Service. *Proposal for a regulation laying down the rules to prevent and combat child sexual abuse: Complementary impact assessment*. PE 740.248. 2023. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf (besucht am 15.04.2024).

Europäische Kommission. *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität*. COM(2021) 281 final. 3. Juni 2021.

Europäische Union. *Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG*. Amtsblatt der Europäischen Union L 257/73. 23. Juli 2014.

Fanta, Alexander. „How a Hollywood star lobbies the EU for more surveillance". In: *Netzpolitik.org* (12. Mai 2022). URL: https://netzpolitik.org/2022/dude-wheres-my-privacy-how-a-hollywood-star-lobbies-the-eu-for-more-surveillance (besucht am 15.04.2024).

Fenner, Dagmar. „Angewandte Ethik zwischen Theorie und Praxis. Systematische Reflexionen zum Theorie-Praxis-Verhältnis der jungen Disziplin". In: *Zeitschrift für philosophische Forschung* 63.1 (2009), S. 99–121.

– *Einführung in die Angewandte Ethik*. Tübingen: Narr Francke Attempto Verlag, 2010.

– *Ethik: Wie soll ich handeln?*. 2. Aufl. Tübingen: Narr Francke Attempto Verlag, 2020.

Ferran, Lee. „Ex-NSA Chief: 'We Kill People Based on Metadata'". In: *ABC News* (12. Mai 2014). URL: https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata (besucht am 15.04.2024).

Filipović, Alexander. „Angewandte Ethik: Grundbegriffe der Kommunikations- und Medienethik (Teil 2)". In: *Soziale Kommunikation im Wandel: 50 Jahre Medienethik und Kommunikation in Kirche und Gesellschaft*. Hrsg. von Klaus-Dieter Altmeppen, Alexander Filipović und Renate Hackel-de Latour. Baden-Baden: Nomos, 2017, S. 122–128.

Fischer, Peter. *Einführung in die Ethik*. München: Wilhelm Fink Verlag, 2003.

Fischermann, Thomas. „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).

Foucault, Michael. *Discipline and Punish: The Birth of the Prison*. 2. Aufl. New York: Vintage Books, 1995.

Freeh, Louis J. *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).

Freeman, Michael. *Human Rights*. 2. Aufl. Cambridge und Malden: Polity Press, 2013.

Fremuth, Michael Lysander. *Menschenrechte: Grundlagen und Dokumente*. Wien und Berlin: Verlag Österreich und Berliner Wissenschafts-Verlag, 2020.

Friedman, William F. *The Index of Coincidence and Its Application to Cryptography*. Riverbank Publications 22. Paris: L. Fournier, 1922.

Fritzsche, K. Peter. *Menschenrechte: Eine Einführung mit Dokumenten*. 3. Aufl. Paderborn: Ferdinand Schöningh, 2016.

Gardner, Martin. „Mathematical Games: A new kind of cipher that would take millions of years to break". In: *Scientific American* (Aug. 1977), S. 120–124.

Gartner, Richard. *Metadata: Shaping Knowledge from Antiquity to the Semantic Web*. Cham: Springer, 2016.

Gasser, Urs u. a. *Don't Panic: Making Progress on the "Going Dark" Debate*. Berkman Center for Internet & Society at Harvard University, 1. Feb. 2016. URL: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (besucht am 15.04.2024).

Gathen, Joachim von zur. *CryptoSchool*. Berlin und Heidelberg: Springer, 2015.

Gillespie, Tarleton. „Engineering a principle: 'End-to-End' in the design of the internet". In: *Social Studies of Science* 36.3 (2006), S. 427–457.

Goldsmith, Jack und Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. Taschenbuchausgabe. Oxford und New York: Oxford University Press, 2008.

Goode, Luke. „Anonymous and the Political Ethos of Hacktivism". In: *Popular Communication* 13.1 (2015), S. 74–86.

Grasselli, Federico. *Quantum Cryptography: From Key Distribution to Conference Key Agreement*. Cham: Springer, 2021.

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

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Penguin Books, 2014.

Griffin, James. *On Human Rights*. Oxford und New York: Oxford University Press, 2008.

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

Hacking, Ian. „Introductory Essay". In: Kuhn, Thomas S. *The Structure of Scientific Revolutions*. 4. Aufl. Chicago und London: The University of Chicago Press, 2012, S. vii–xxxvii.

Halaburda, Hanna, Miklos Sarvary und Guillaume Haeringer. *Beyond Bitcoin: Economics of Digital Currencies and Blockchain Technologies*. 2. Aufl. Cham: Palgrave Macmillan, 2022.

Hallgren, Sean und Ulrich Vollmer. „Quantum computing". In: *Post-Quantum Cryptography*. Hrsg. von Daniel J. Bernstein, Johannes Buchmann und Erik Dahmen. Berlin und Heidelberg: Springer, 2009, S. 15–34.

Hasian Jr., Marouf, Sean Lawson und Megan D. McFarlane. *The Rhetorical Invention of America's National Security State*. Lanham u. a.: Lexington Books, 2015.

Heinemann, Marcus. *Grundrechtlicher Schutz informationstechnischer Systeme: Unter besonderer Berücksichtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Berlin: Duncker & Humblot, 2015.

Hill, Lester S. „Cryptography in an Algebraic Alphabet". In: *The American Mathematical Monthly* 36.6 (1929), S. 306–312.
Hilpert, Konrad. *Ethik der Menschenrechte: Zwischen Rhetorik und Verwirklichung*. Paderborn: Ferdinand Schöningh, 2019.
Hodges, Andrew. *Alan Turing: The Enigma*. Princeton und Oxford: Princeton University Press, 2014.
Homeister, Matthias. *Quantum Computing verstehen: Grundlagen – Anwendungen – Perspektiven*. 6. Aufl. Wiesbaden: Springer Vieweg, 2022.
Hoofnagle, Chris J. und Simson J. Garfinkel. *Law and Policy for the Quantum Age*. Cambridge: Cambridge University Press, 2022.
Horton, John. „Self-Censorship". In: *Res Publica* 17.1 (2011), S. 91–106.
Hughes, Eric. *A Cypherpunk's Manifesto*. 1993. URL: https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt (besucht am 15.04.2024).
Human Rights Council. *The promotion, protection and enjoyment of human rights on the Internet*. A/HRC/RES/20/8. 2012.
– *The right to privacy in the digital age*. A/HRC/RES/42/15. 2019.
Humbach, John A. „Privacy and the Right of Free Expression". In: *First Amendment Law Review* 11.1 (2012), S. 16–89.
Hurlburt, George u. a. „Security or Privacy? A Matter of Perspective". In: *Computer* 47.11 (2014), S. 94–98.
Höffe, Otfried. *Ethik: Eine Einführung*. München: Verlag C. H. Beck, 2013.
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).
James, Ioan. „Obituary: Claude Elwood Shannon 1916–2001". In: *Bulletin of the London Mathematical Society* 46.2 (2014), S. 435–440.
Jarvis, Craig. *Crypto Wars: The Fight for Privacy in the Digital Age. A Political History of Digital Encryption*. Boca Raton: CRC Press, 2021.
– „Cypherpunk ideology: Objectives, profiles, and influences (1992–1998)". In: *Internet Histories* 6.3 (2021), S. 315–342.
Jing, Jin, Abdelsalam Sumi Helal und Ahmed Elmagarmid. „Client-server computing in mobile environments". In: *ACM Computing Surveys* 31.2 (1999), S. 117–157.
Jordan, Tim. *Information Politics: Liberation and Exploitation in the Digital Society*. London: Pluto Press, 2015.
Jočienė, Danutė. „Freedom of expression and the right to privacy". In: *Teisė* 38 (2001), S. 7–19.
Kahn, David. *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943*. Überarbeitete Auflage. London: Frontline Books, 2012.
– *The Codebreakers: The Story of Secret Writing*. Überarbeitete Version. New York: Scribner, 1996.
– „The Significance of Codebreaking and Intelligence in Allied Strategy and Tactics". In: *Cryptologia* 1.3 (1977), S. 209–222.
Kalai, Gil. *The Quantum Computer Puzzle (Expanded Version)*. 2016. arXiv: 1605.00992v1. URL: http://arxiv.org/pdf/1605.00992v1 (besucht am 15.04.2024).

– *Three Puzzles on Mathematics, Computation, and Games*. 2018. arXiv: 1801.02602v1. URL: http://arxiv.org/pdf/1801.02602v1 (besucht am 15.04.2024).
Kant, Immanuel. *Grundlegung zur Metaphysik der Sitten*. Hrsg. von Bernd Kraft und Dieter Schönecker. Hamburg: Felix Meiner Verlag, 1999.
Kardefelt-Winther, Daniel u. a. *Encryption, Privacy and Children's Right to Protection from Harm*. Innocenti Working Paper 2020-14. UNICEF, 2020. URL: https://www.unicef.org/innocenti/media/3446/file/UNICEF-Encryption-Privacy-Right-Protection-From-Harm-2020.pdf (besucht am 15.04.2024).
Katz, Jonathan und Yehuda Lindell. *Introduction to Modern Cryptography*. 2. Aufl. Boca Raton: CRC Press, 2015.
Kaye, David. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/29/32. Human Rights Council, 2015.
Kelber, Ulrich. *Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur öffentlichen Anhörung des Ausschusses für Digitales des Deutschen Bundestages am Mittwoch, 1. März 2023, 14:00 bis 16:00 Uhr zum Thema „Chatkontrolle"*. 28. Feb. 2023. URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_Chatkontrolle.pdf?__blob=publicationFile&v=1 (besucht am 15.04.2024).
Kerckhoffs, Auguste. „La Cryptographie Militaire: Première partie". In: *Journal des sciences militaires* IX (Jan. 1883), S. 5–38.
– „La Cryptographie Militaire: Seconde Partie". In: *Journal des sciences militaires* IX (Feb. 1883), S. 161–191.
Kirchschläger, Peter G. „Das Prinzip der Verletzbarkeit als Begründungsweg der Menschenrechte". In: *Freiburger Zeitschrift für Philosophie und Theologie* 62 (2015).
– *Wie können Menschenrechte begründet werden? Ein für religiöse und säkulare Menschenrechtskonzeptionen anschlussfähiger Ansatz*. Münster: Lit Verlag, 2013.
Koops, Bert-Jaap und Eleni Kosta. „Looking for Some Light Through the Lens of 'Cryptowar' History: Policy Options for Law Enforcement Authorities Against ‚Going Dark'". In: *Computer Law & Security Review* 34 (2018), S. 890–900.
Kuhn, Thomas S. *The Structure of Scientific Revolutions*. 4. Aufl. Chicago und London: The University of Chicago Press, 2012.
La Rue, Frank. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/23/40. Human Rights Council, 2013.
Laaff, Meike. „Wir haben ja nichts gegen Verschlüsselung. Aber". In: *ZEIT Online* (12. Mai 2022). URL: https://www.zeit.de/digital/2022-05/chatkontrolle-eu-kinder-sexualisierte-gewalt-chatverschluesselung-datenschutz (besucht am 15.04.2024).
Landau, Susan. *Surveillance or Security: The Risks Posed by New Wiretapping Technologies*. Cambridge, MA, und London: MIT Press, 2010.
– „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).

Legal Service of the Council of the European Union. *Opinion of the Legal Service*. 8787/23. 26. Apr. 2023. URL: https://data.consilium.europa.eu/doc/document/ST-8787-2023-INIT/en/pdf (besucht am 15.04.2024).

Lessig, Lawrence. *Code: And Other Laws Of Cyberspace*. New York: Basic Books, 1999.

– *Code: Version 2.0*. New York: Basic Books, 2006.

– „The Architecture of Privacy: Remaking Privacy in Cyberspace". In: *Vanderbilt Journal of Entertainment & Technology Law* 1.1 (1999), S. 56–65.

– „The New Chicago School". In: *The Journal of Legal Studies* 27.S2 (1998), S. 661–691.

– „The Zones of Cyberspace". In: *Stanford Law Review* 48.5 (1996), S. 1403–1411.

Levinson, Daryl J. „Collective Sanctions". In: *Stanford Law Review* 56.2 (2003), S. 345–428.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age*. New York: Penguin Books, 2002.

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

– *Hackers: Heros of the Computer Revolution*. Ausgabe zum 25-jährigen Jubiläum. Beijing u. a.: O'Reilly, 2010.

Limniotis, Konstantinos. „Cryptography as the Means to Protect Fundamental Human Rights". In: *Cryptography* 5.4 (2021).

Lo, Hoi-Kwong und Hoi Fung Chau. „Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances". In: *Science* 283.5410 (1999), S. 2050–2056.

Lucas, George. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*. New York: Oxford University Press, 2017.

Lunkeit, Armin und Wolf Zimmer. *Security by Design: Security Engineering informationstechnischer Systeme*. Berlin und Heidelberg: Springer Vieweg, 2021.

Lyon, David. *Surveillance society: Monitoring everyday life*. Buckingham und Philadelphia: Open University Press, 2005.

– *Surveillance Studies: An Overview*. Cambridge und Malden: Polity Press, 2008.

– *The Electronic Eye: The Rise of Surveillance Society*. Cambridge: Polity Press, 1994.

MacIntyre, Alasdair. *After Virtue: A Study in Moral Theory*. 3. Aufl. Notre Dame: University of Notre Dame Press, 2007.

Macnish, Kevin. „An End to Encryption? Surveillance and Proportionality in the Crypto-Wars". In: *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*. Hrsg. von Adam Henschke u. a. Cham: Springer, 2021, S. 155–173.

Mann, Steve. „'Sousveillance': Inverse Surveillance in Multimedia Imaging". In: *Proceedings of the 12th annual ACM international conference on multimedia*. MULTIMEDIA '04. New York, NY, USA: Association for Computing Machinery, 2004, S. 620–627.

Manne, Robert. „The Snowden files". In: *The Monthly* (Sep. 2014). URL: https://www.themonthly.com.au/issue/2014/september/1409493600/robert-manne/snowden-files (besucht am 15.04.2024).

Manokha, Ivan. „Surveillance, Panopticism, and Self-Discipline in the Digital Age". In: *Surveillance and Society* 16.2 (2018), S. 219–237.

Marx, Gary T. *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago und London: The University of Chicago Press, 2016.

Mattelart, Armand. *The Globalization of Surveillance: The Origin of the Securitarian Order*. Cambridge und Malden: Polity Press, 2010.

May, Timothy C. *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).

– *The Cyphernomicon*. 1994. URL: https://nakamotoinstitute.org/static/docs/cyphernomicon.txt (besucht am 15.04.2024).

McKay, Brendan u. a. „Solving the Bible Code Puzzle". In: *Statistical Science* 14.2 (1999), S. 150–173.

Meaker, Morgan. „Europe's Moral Crusader Lays Down the Law on Encryption". In: *Wired* (11. Mai 2023). URL: https://www.wired.co.uk/article/europes-ylva-johansson-lays-down-the-law-on-encryption (besucht am 15.04.2024).

Meineck, Sebastian. „Das sagen Kinderschutz-Organisationen zur Chatkontrolle". In: *Netzpolitik.org* (20. Mai 2022). URL: https://netzpolitik.org/2022/massenueberwachung-das-sagen-kinderschutz-organisationen-zur-chatkontrolle (besucht am 15.04.2024).

Meineck, Sebastian, Anna Biselli und Markus Reuter. „So führt EU-Kommissarin Ylva Johansson die Öffentlichkeit in die Irre". In: *Netzpolitik.org* (10. Feb. 2023). URL: https://netzpolitik.org/2023/chatkontrolle-so-fuehrt-eu-kommissarin-ylva-johansson-die-oeffentlichkeit-in-die-irre/#netzpolitik-pw (besucht am 15.04.2024).

Meister, Andre. „EU-Rat verschiebt Abstimmung über Chatkontrolle". In: *Netzpolitik.org* (21. Sep. 2023). URL: https://netzpolitik.org/2023/internes-protokoll-eu-rat-verschiebt-abstimmung-ueber-chatkontrolle/ (besucht am 15.04.2024).

– „Immer mehr EU-Staaten gegen unverhältnismäßige Chatkontrolle". In: *Netzpolitik.org* (23. Nov. 2023). URL: https://netzpolitik.org/2023/internes-protokoll-immer-mehr-eu-staaten-gegen-unverhaeltnismaessige-chatkontrolle/ (besucht am 15.04.2024).

– „Politiker fordern Ausweitung der Chatkontrolle auf andere Inhalte". In: *Netzpolitik.org* (6. Okt. 2023). URL: https://netzpolitik.org/2023/ueberwachung-politiker-fordern-ausweitung-der-chatkontrolle-auf-andere-inhalte (besucht am 15.04.2024).

– „Verpflichtende Chatkontrolle vorerst gescheitert". In: *Netzpolitik.org* (13. Dez. 2023). URL: https://netzpolitik.org/2023/etappensieg-verpflichtende-chatkontrolle-vorerst-gescheitert/ (besucht am 15.04.2024).

Menezes, Alfred J., Paul C. van Oorschot und Scott A. Vanstone. *Handbook of Applied Cryptography*. Boca Raton: CRC Press, 1997.

Michael, James Bret, Richard Kuhn und Jeffrey Voas. „Security or Privacy: Can You Have Both?“ In: *Computer* 53.9 (2020), S. 20–30.

Minh, Dang u. a. „Explainable artificial intelligence: a comprehensive review“. In: *Artificial Intelligence Review* 55.5 (2022), S. 3503–3568.

Moore, Ciara u. a. „Practical homomorphic encryption: A survey“. In: *IEEE International Symposium on Circuits and Systems (ISCAS)*. 2014, S. 2792–2795.

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

Mosca, Michele. „Cybersecurity in an Era with Quantum Computers: Will We Be Ready?“ In: *IEEE Security and Privacy* 16.5 (2018), S. 38–41.

Murray, Daragh u. a. „The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe“. In: *Journal of Human Rights Practice* (2023), huad020.

Nabeel, Mohamed. „The Many Faces of End-to-End Encryption and Their Security Analysis“. In: *IEEE International Conference on Edge Computing (EDGE)*. 2017, S. 252–259.

Naccache, David, Peter Y. A. Ryan und Jean-Jacques Quisquater. „Preface“. In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Hrsg. von Peter Y. A. Ryan, David Naccache und Jean-Jacques Quisquater. Berlin und Heidelberg: Springer, 2016, S. IX–X.

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

National Institute of Standards and Technology. *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. 5. Juli 2022. URL: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (besucht am 15.04.2024).

– *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. (FIPS PUB 202). Gaithersburg, Aug. 2015. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf (besucht am 15.04.2024).

National Security Agency. *Transition 2001*. Dez. 2000. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3700340/National-Security-Agency-Transition-2001.pdf (besucht am 15.04.2024).

Neukirch, Ralf und Wolf Wiedmann-Schmidt. „‚Es geht um viele Kinder, die wir retten können‘“. In: *Der Spiegel* (10. Feb. 2023). URL: https://www.spiegel.de/politik/deutschland/eu-kommissarin-ylva-johansson-ueber-missbrauch-im-netz-es-geht-um-viele-kinder-die-wir-retten-koennen-a-63bdbf05-f201-4d03-abfd-fd12a83a2d62 (besucht am 15.04.2024).

Ni Loideain, Nora. „EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era“. In: *Media and Communication* 3.2 (2015).

Ogburn, Monique, Claude Turner und Pushkar Dahal. „Homomorphic Encryption“. In: *Procedia Computer Science* 20 (2013), S. 502–509.

Oorschot, Paul C. van. *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin*. Cham: Springer, 2021.

Pascual, Manuel G. „Fighting pedophilia at the expense of our privacy: The EU rule that could break the internet". In: *El País* (17. Okt. 2023). URL: https://english.elpais.com/technology/2023-10-17/fighting-pedophilia-at-the-expense-of-our-privacy-the-eu-rule-that-could-break-the-internet.html (besucht am 15.04.2024).

Pauer-Studer, Herlinde. *Einführung in die Ethik*. 3. Aufl. Wien: Facultas, 2020.

Penney, Jonathon W. „Internet surveillance, regulation, and chilling effects online: A comparative case study". In: *Internet Policy Review* 2.6 (2017), S. 1–39.

– „Understanding Chilling Effects". In: *Minnesota Law Review* 106 (2022), S. 1451–1530.

Perlroth, Nicole. „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).

Pieper, Annemarie. *Einführung in die Ethik*. 2. Aufl. Tübingen: Francke Verlag, 1991.

Podgorelec, Blaž, Lukas Alber und Thomas Zefferer. „What is a (digital) identity wallet? A systematic literature review". In: *IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*. 2022, S. 809–818.

Pomerantz, Jeffrey. *Metadata*. Cambridge, MA, und London: MIT Press, 2015.

Portnoy, Erica. *Why Adding Client-Side Scanning Breaks End-To-End Encryption*. Electronic Frontier Foundation. 1. Nov. 2019. URL: https://www.eff.org/de/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption (besucht am 15.04.2024).

Preskill, John. „Quantum Computing in the NISQ era and beyond". In: *Quantum* 2 (2018), Art. Nr. 79.

Prevezianou, Maria F. „WannaCry as a Creeping Crisis". In: *Understanding the Creeping Crisis*. Hrsg. von Arjen Boin, Magnus Ekengren und Mark Rhinard. Cham: Palgrave Macmillan, 2021, S. 37–50.

Quante, Michael. *Einführung in die Allgemeine Ethik*. 2. Aufl. Darmstadt: WBG, 2006.

Ramiro, André und Ruy de Queiroz. „Cypherpunk". In: *Internet Policy Review* 11.2 (2022).

Rau, Franziska und Esther Menhard. „Wie die Chatkontrolle EU-weit Wellen schlägt". In: *Netzpolitik.org* (15. Sep. 2022). URL: https://netzpolitik.org/2022/plaene-der-kommission-wie-die-chatkontrolle-eu-weit-wellen-schlaegt/ (besucht am 15.04.2024).

Ray, LaPierre. *Introduction to Quantum Computing*. Cham: Springer, 2021.

Renner, Renato. „Security of Quantum Key Distribution". Dissertation No. 16242. Zürich: ETH Zürich, 2005.

Rescher, Nikolas. „Leibniz's Machina Deciphratoria: A Seventeenth-Century Proto-Enigma". In: *Cryptologia* 38.2 (2014), S. 103–115.

Reuter, Markus. „EU-Kommission schaltet irreführende Werbung für Chatkontrolle auf X". In: *Netzpolitik.org* (13. Okt. 2023). URL: https://netzpolitik.org/2023/politisches-mikrotargeting-eu-kommission-schaltet-irrefuehrende-werbung-fuer-chatkontrolle-auf-x (besucht am 15.04.2024).

Reuter, Markus. „Gesetzesvorhaben in EU, UK und den USA gefährden Verschlüsselung". In: *Netzpolitik.org* (2022). URL: https://netzpolitik.org/2022/crypto-wars-gesetzesvorhaben-in-eu-uk-und-den-usa-gefaehrden-verschluesselung (besucht am 15.04.2024).

Richard, Laurent und Sandrine Rigaud. *Pegasus: The Story of the World's Most Dangerous Spyware*. New York: Henry Holt and Co., 2023.

Ricken, Friedo. *Allgemeine Ethik*. 4. Aufl. Stuttgart: Verlag W. Kohlhammer, 2003.

Rid, Thomas. *Rise of the Machines: The Lost History of Cybernetics*. Melbourne und London: Scribe, 2016.

Riebe, Thea. *Technology Assessment of Dual-Use ICTs: How to Assess Diffusion, Governance and Design*. Wiesbaden: Springer Vieweg, 2023.

Riebe, Thea u. a. „U.S. Security Policy: The Dual-Use Regulation of Cryptography and its Effects on Surveillance". In: *European Journal for Security Research* 7.1 (2022), S. 39–65.

Rip, Arie. „Technology Assessment". In: *International Encyclopedia of the Social & Behavioral Sciences*. Hrsg. von James D. Wright. 2. Aufl. Bd. 24. Amsterdam: Elsevier, 2015, S. 125–128.

Rivest, Ron L., Adi Shamir und Leonard Adleman. „A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Communications of the ACM* 21.2 (1978), S. 120–126.

Rogaway, Phillip. *The Moral Character of Cryptographic Work*. 2015. Cryptology ePrint Archive: 2015/1162. URL: https://eprint.iacr.org/2015/1162 (besucht am 15.04.2024).

Rogers, Richard. „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.

Rorty, Richard. *Truth and Progress: Philosophical Papers*. Cambridge: Cambridge University Press, 1998.

Ruiz, Blanca R. *Privacy in Telecommunications: A European and an American Approach*. Den Haag: Kluwer Law International, 1997.

Russell, Andrew L. „'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.

Saltzer, Jerry H., 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.

– „End-to-End Arguments in System Design". In: *ACM Transactions in Computer Systems* 2.4 (1984), S. 277–288.

Scheuerman, William E. „Whistleblowing as civil disobedience: The case of Edward Snowden". In: *Philosophy & Social Criticism* 40.7 (2014), S. 609–628.

Schmid, Kathrin. „Im Dilemma zwischen Daten- und Kinderschutz". In: *Tagesschau* (14. Nov. 2023). URL: https://www.tagesschau.de/ausland/europa/chatkontrolle-eu-kindesmissbrauch-100.html (besucht am 15.04.2024).

Schulz, Wolgang und Joris van Hoboken. *Human rights and encryption*. Paris: UNESCO Publishing, 2016. URL: https://unesdoc.unesco.org/ark:/48223/pf0000246527 (besucht am 15.04.2024).

Schulze, Matthias. „From Cyber-Utopia to Cyber-War: Normative Change in Cyberspace". Dissertation. Jena, 2018.

Shannon, Claude E. „A Mathematical Theory of Communication". In: *The Bell System Technical Journal* 27.3 (1948), S. 379–423.

– „Communication Theory of Secrecy Systems". In: *The Bell System Technical Journal* 28.4 (1949), S. 656–715.

Sharif, Amir u. a. „The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes". In: *Applied Sciences* 12.24 (2022), Art. Nr. 12679.

Shih, Frank Y. *Digital Watermarking and Steganography: Fundamentals and Techniques*. 2. Aufl. Boca Raton: CRC Press, 2017.

Shor, Peter W. „Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *IEEE Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, S. 124–134.

Singh, Simon. *Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets*. 17. Aufl. München: dtv, 2022.

– *The Code Book: The Secret History of Codes and Codebreaking*. Taschenbuchausgabe. London: Fourth Estate, 2000.

Sinha, Alok. „Client-server computing". In: *Communications of the ACM* 35.7 (1992), S. 77–98.

Snowden, Edward. *Permanent Record*. London: Pan Books, 2019.

Solove, Daniel J. „A Taxonomy of Privacy". In: *University of Pennsylvania Law Review* 154.3 (2006), S. 477–564.

– „'I've Got Nothing to Hide' and Other Misunderstandings of Privacy". In: *San Diego Law Review* 44.1 (2007), S. 745–772.

– *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven und London: Yale Univeristy Press, 2011.

Spencer, Shaun B. „Security versus Privacy: Reframing the Debate". In: *Denver University Law Review* 79.4 (2002), S. 519–521, 554, 571–573.

Stalla-Bourdillon, Sophie, Joshua Phillips und Mark D. Ryan. *Privacy vs. Security*. London u. a.: Springer, 2014.

Stoycheff, Elizabeth u. a. „Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects". In: *New Media & Society* 21.3 (2019), S. 602–619.

The White House Office of the Press Secretary. „Statement by the President". San Jose, CA, 7. Juni 2013. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president (besucht am 15.04.2024).

Toulson, Roger. „Freedom of Expression and Privacy". In: *The Law Teacher* 41.2 (2007), S. 139–154.

Traylor, John Mylan. „Shedding Light on the 'Going Dark' Problem and the Encryption Debate". In: *University of Michigan Journal of Law Reform* 50.489 (2016).

Turing, Alan M. „I.—Computing Machinery and Intelligence". In: *Mind* LIX.236 (1950), S. 433–460.

Türk, Volker. *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*. A/HRC/51/17. United Nations Human Rights Council, 2022.
– *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*. A/HRC/39/29. United Nations Human Rights Council, 2018.
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).
United States Senate. *Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard*. Staff Report of the Senate Selected Committee on Intelligence. Washington: U.S. Government Printing Office, Apr. 1978. URL: https://www.intelligence.senate.gov/sites/default/files/publications/95nsa.pdf (besucht am 15.04.2024).
Vella, Veronica. „Is There a Common Understanding of Dual-Use? The Case of Cryptography". In: *Strategic Trade Review* 3.4 (2017), S. 103–122.
Wagner, R. Polk. „On Software Regulation". In: *Southern California Law Review* 78.2 (2005), S. 457–520.
Webb, Maureen. *Coding Democracy: How Hackers Are Disrupting Power, Surveillance, and Authoritarianism*. Cambridge, MA, und London: MIT Press, 2020.
Whitaker, Reg. *The End of Privacy: How Total Surveillance Is Becoming Reality*. New York: The New Press, 1999.
Williams, Hugh. *An Interview with Martin Hellman. Recipient of the 2015 ACM Turing Award*. Palo Alto, 19. Mai 2017. URL: https://amturing.acm.org/pdf/HellmanTuringTranscript.pdf (besucht am 15.04.2024).
Williams, John Allen, Stephen J. Cimbala und Sam C. Sarkesian. *US National Security: Policymakers, Processes, and Politics*. 6. Aufl. Boulder und London: Lynne Rienner Publishers, 2022.
Wissenschaftliche Dienste des Deutschen Bundestages. *„Chatkontrolle" – Analyse des Verordnungsentwurfs 2022/0155 (COD) der EU-Kommission*. WD 10 – 3000 – 026/22. 2022. URL: https://www.bundestag.de/resource/blob/914580/9eba1ff3a5daa7708fca92e3184a1ae3/WD-10-026-22-pdf-data.pdf (besucht am 15.04.2024).
Woerlein, Andreas H. „EU-Kommission: Gesetzesvorschlag im Kampf gegen Kindesmissbrauch – kommt die Chatkontrolle?" In: *ZD-Aktuell* 01251 (2022).
Wolf, Ramona. *Quantum Key Distribution: An Introduction with Exercises*. Cham: Springer, 2021.
Wolff, Jonathan. *An Introduction to Moral Philosophy*. New York und London: W. W. Norton & Company, 2018.
Woods, Kerri. *Human Rights*. Basingstoke und New York: Palgrave Macmillan, 2014.
Wätjen, Dietmar. *Kryptographie: Grundlagen, Algorithmen, Protokolle*. Wiesbaden: Springer Vieweg, 2018.
Zimba, Aaron und Mumbi Chishimba. „On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems". In: *European Journal for Security Research* 4.1 (2019), S. 3–31.

Zimmermann, Phil. *PGP: Source Code and Internals*. Cambridge, MA: MIT Press, 1995.

– *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).

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

Zuiderveen Borgesius, Frederik J. und Wilfred Steenbruggen. „The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust". In: *Theoretical Inquiries in Law* 20.1 (2019), S. 291–322.

Zwart, Melissa de. „Privacy for the weak, transparency for the powerful*". In: *Comparative Defamation and Privacy Law*. Hrsg. von Andrew T. Kenyon. Cambridge: Cambridge University Press, 2016, S. 224–245.