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.