Einführung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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