Freie Universität Berlin

Open C3S
Open Competence Center for Cyber Security

Zertifikatsprogramm

Informationsethik und Datenschutz für Ermittler und Verteidiger

Autoren:

Dr. Werner Kogge

Dr. Sandro Gaycken

Freie Universität Berlin

Modul 3

Informationsethik und Datenschutz für Ermittler und Verteidiger

---

Studienbrief 1: Einführung in die Informationsethik

Studienbrief 2: Informationsethik und Sicherheitsrationalität

Studienbrief 3: Einführung in den Datenschutz

Studienbrief 4: Wert und Strukturen der Sicherheit und Freiheit in Cybercrime

---

Autoren:

Dr. Werner Kogge

Dr. Sandro Gaycken

---

1. Auflage

Freie Universität Berlin

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung, und Forschung unter dem Förderkennzeichen 16OH11072 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Freie Universität Berlin
Fachbereich Mathematik und Informatik
Takustraße 9
14195 Berlin

1. Auflage (12. November 2015)

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Übung	Ü

II. Modullehrziele

Der erste Studienbrief gibt Ihnen einen Überblick über das Thema Ethik und über Grundfragen eines Spezialgebietes der Ethik, nämlich die Informationsethik. Sie erfahren, was mit dem Begriff Ethik bezeichnet wird und erhalten Orientierung darüber, in welchem Verhältnis Ethik zu Moral und Recht steht. Dabei liegt ein Schwerpunkt auf ethischen Fragen im beruflichen Umfeld. Indem Ihnen verschiedene Ansätze der philosophischen Ethik vermittelt werden, sollen Sie auch in die Lage versetzt werden, unterschiedliche Typen ethischer Argumentation zu identifizieren. Ein Ziel ist schließlich, dass Sie vor diesem Hintergrund Problemstellungen der Technik- und Informationsethik selbständig behandeln können. Dieses Modul wird dabei den Konflikt zwischen Freiheit und Sicherheit genauer identifizieren. Dazu wird er folgende Themen bearbeiten:

1. Sicherheit als Wert
2. Prinzipien der Sicherheitsrationalität
3. Sicherheit und Freiheit
4. Freiheiten in der Informationsethik
    a) Menschenrechte in digitalen Welten
    b) Freiheit von Information und Wissen
    c) Freiheit von Kommunikation

Mit diesen Kenntnissen und Fähigkeiten sind Sie in der Lage, Probleme der Informationsethik zu verstehen, den Konflikt zwischen Sicherheit und Freiheit zu formulieren, Rahmenbedingungen und die Folgen des Handelns im Informationsraum abschätzen zu können, sowohl gesamtgesellschaftlich als auch bezogen auf bestimmte, enger umrissene Problemstellungen. So werden auch Regulierungen für Sie leichter verständlich. Zukünftige Regulierungen werden besser absehbar.

Studienbrief 1 Einführung in die Informationsethik

1.1 Lernziele

Was wird Ihnen vermittelt?

Dieser Studienbrief gibt Ihnen einen Überblick über das Thema Ethik und über Grundfragen eines Spezialgebietes der Ethik, nämlich die Informationsethik. Sie erfahren, was mit dem Begriff Ethik bezeichnet wird und erhalten Orientierung darüber, in welchem Verhältnis Ethik zu Moral und Recht steht. Dabei liegt ein Schwerpunkt auf ethischen Fragen im beruflichen Umfeld. Indem Ihnen verschiedene Ansätze der philosophischen Ethik vermittelt werden, sollen Sie auch in die Lage versetzt werden, unterschiedliche Typen ethischer Argumentation zu identifizieren. Ein Ziel ist schließlich, dass Sie vor diesem Hintergrund Problemstellungen der Technik- und Informationsethik selbständig behandeln können.

1.2 Advanced Organizer

Für den Studienbrief 1 Einführung in die Informationsethik werden keine Vorkenntnisse vorausgesetzt. Es werden grundlegende Prinzipien und Zusammenhänge erklärt, um das Verständnis der folgenden Studienbriefe zu erleichtern.

1.3 Moral, Ethik und Recht

Was ist Moral?

Stellen Sie sich vor, eine größere Anzahl Schiffsbrüchiger erreicht eine unbewohnte Insel. Ausgehungert und dem Verdursten nahe stürzen sich

die Passagiere auf alles Trink- und Essbare, das Sie finden können. Einige allerdings geben zuerst ihren Kindern, andere beginnen bald, die Alten und Kranken zu versorgen. Wieder andere teilen alles, was sie finden und geben den Menschen in ihrer Umgebung ab. Bald wird es bei einigen üblich, alle gefundene und erjagte Nahrung in ihrer Mitte zu sammeln und zu gleichen Teilen an die Mitglieder der Gruppe abzugeben. In den verschiedenen Familien und Gruppen der Schiffsbrüchigen bilden sich verschiedene Umgangsformen aus. Diese Umgangsformen unterscheiden sich voneinander. Gemeinsam unterscheiden sie sich allerdings vom Anfangszustand kurz nach der Landung dadurch, dass das Handeln hier nun Regeln folgt, die mit Auffassungen darüber verbunden sind, was gut und gerecht ist. Die Schiffsbrüchigen, die solchen Regeln folgen, verhalten sich moralisch.

D

Definition 1.1: Moralisch

Moralisch ist ein Handeln, das sich an in einer Gruppe geteilten Auffassungen darüber orientiert, was gut und gerecht ist.

Das Adjektiv „moralisch“ bezieht sich zunächst auf die Weise, in der etwas getan wird. Genauer: Es bezieht sich darauf, woran sich jemand, der handelt, orientiert. Abgeleitet davon können Überzeugungen und sprachliche Äußerungen als moralisch bzw. unmoralisch bezeichnet werden.

Schwieriger ist die Bestimmung des Substantivs „Moral“. Sehen Sie sich die Definition im Duden an:

D

Definition 1.2: Moral

„Gesamtheit von ethisch-sittlichen Normen, Grundsätzen, Werten, die das zwischenmenschliche Verhalten einer Gesellschaft regulieren, die von ihr als verbindlich akzeptiert werden.“ (10)

Die Schwierigkeit in dieser Definition besteht darin, dass in ihr weitere erklärungsbedürftige Wörter verwendet werden. Zu klären ist vor allem, was mit ëthisch-sittlich"gemeint ist.

Kehren wir dazu noch einmal zurück zu den Schiffsbrüchigen: Wir können uns vorstellen, dass die Leute dort ihre Auffassungen darüber, was im Handeln gut und gerecht ist, in vielen Situationen sprachlich vermitteln und verhandeln: „Teile gerecht!“; „Man gibt zuerst den Ältesten.“; „Wer

am meisten arbeitet, soll auch am meisten essen.“ Solche Anweisungen und Regeln können Nachfragen und Widerspruch hervorrufen. Nachfragen und Widerspruch erfordern wiederum Begründungen und Rechtfertigungen. Unterschiedliche Begründungen und Rechtfertigungen können aber einander widersprechen. So entsteht in vielen Situationen der Bedarf, in einer Gemeinschaft Einigkeit darüber zu erlangen, was als gut und gerecht gilt oder zumindest: Klarheit darüber zu gewinnen, was, unter welchen Umständen und für wen zu gelten hat.

Für gewöhnlich beschränken sich solche Rechtfertigungen und Begründungen darauf zu erklären, es sei gut und gerecht, z.B. den Notleidenden zu helfen, die Alten zu ehren, für die Kinder zu sorgen. So zu handeln sei üblich, es entspreche Brauch und Sitte in der Gemeinschaft.

Das Verhältnis von Moral und Ethik

An dieser Stelle können wir nun verdeutlichen, in welchem Verhältnis die Begriffe Moral und Ethik zueinander stehen: Während mit dem Wort Moral das an Auffassungen von gut und gerecht orientierte Handeln verstanden wird, bezieht sich das Wort Ethik auf Überlegungen, Diskussionen und Verhandlungen darüber, was als gut und gerecht zu gelten habe und aus welchem Grund. Kurz: Moral betrifft Handeln, Ethik das Nachdenken über Handeln. „Die Ethik ist nicht selber Moral, sondern redet über Moral.“ (32, S. 24) In unserem Beispiel: Während sich Moral bei den Schiffsbrüchigen schon früh in ihren Verhaltensweisen zeigte, bildeten sie Ethiken erst aus, als sie über gutes und gerechtes Handeln ausdrücklich nachdachten und diskutierten.

D

Definition 1.3: Ethik

Ethik ist die Thematisierung moralischen Handelns und der mit diesem verbundenen Fragen, Auffassungsunterschiede, Gründe, Rechtfertigungen und Widersprüche.

K

Kontrollaufgabe 1.1: Ethik und Moral

Welches der beiden Adjektive, moralisch oder ethisch, ist in folgenden Sätzen sinnvollerweise einzufügen?

1. Die Firma erstellte nach ausführlicher Diskussion einen Katalog _____ Prinzipien, an denen sich die Mitarbeiter orientieren sollten.

2. Sie handelte spontan in hoch-_____ Weise.

Andere Definitionen von Ethik

In Einführungen und Lehrbüchern zur Ethik finden Sie häufig Begriffsbestimmungen, die Ethik als „Wissenschaft vom moralischen Handeln“ (32, S. 17), als „philosophische Untersuchung des Problembereichs der Moral“ (31, S. 3) oder als „gleichbedeutend mit Moralphilosophie“ (19, S. 9) verstehen. Wenn Sie diese Begriffsbestimmungen mit unserer Definition 1.3 vergleichen, dann sehen Sie, dass mit diesen Bestimmungen deutlich 'höher gegriffen' wird. Definition 1.3 spricht von „Thematisierung“. Eine Thematisierung muss aber nicht sogleich zu einer „Wissenschaft“, zu einer „philosophischen Untersuchung“ oder einer „Moralphilosophie“ ausgebaut werden. Ethik ist keine Spezialdisziplin, für die nur Wissenschaftler und Philosophen zuständig wären. Ethische Überlegungen und Aushandlungen finden überall dort statt, wo Menschen zusammenleben, zusammenarbeiten, ganz allgemein: Wo Menschen ihrem Tun und Lassen Anleitung und Orientierung geben.

E

Exkurs 1.1: Wortgeschichte und philosophische Ethik

Das altgriechische Wort für Brauch und Sitte ist ëthos". Wer sich gemäß Brauch und Sitte verhält, verhält sich „ethikos“. Das deutsche Fremdwort Ethik stammt also aus dem Altgriechischen und bedeutet zunächst nichts anderes als Sitte und Brauch. Ebenso entstammt das Wort Moral einer antiken Quelle. Das lateinische Wort „mos“ (Plural „mores“) bezeichnete ebenfalls Sitte und Brauch. Demgemäß haben römische Gelehrte das griechische Wort „ethos“ mit „mos“ übersetzt. Die Bedeutungen der beiden Worte haben sich dann aber im Verlauf der abendländischen Geistesgeschichte immer mehr unterschieden. Während das Wort Moral sich gleichbleibend auf Sitte und Gebrauch bezog, bezeichnete Ethik eine philosophische Textsorte

(Genre), die in der Tradition der ethischen Schriften des Aristoteles stehen. Philosophinnen und Philosophen denken deshalb, wenn sie das Wort Ethik verwenden, zuerst und zumeist an dieses philosophische Genre und nicht an ethische Fragen und Erwägungen, die wir alle auch im Alltag anstellen. Die Beschränkung des Wortes Ethik auf wissenschaftliche oder philosophische Untersuchungen ist nicht unproblematisch. Denn so kann es scheinen, dass Ethik nur da zu finden sei, wo eine spezielle Technik der Argumentation entwickelt ist. In einer philosophischen *Einführung in die Ethik* lesen wir zum Beispiel: „Die Ethik erörtert alle mit dem Moralischen zusammenhängende Probleme [...], indem sie rein *formal* die Bedingungen rekonstruiert, die erfüllt sein müssen, damit eine Handlung, gleich welchen Inhalt sie im einzelnen haben mag, zu Recht als eine moralische Handlung bezeichnet werden kann.“ (32, S. 24) Eine formale Rekonstruktion ist eine spezielle Technik und deshalb wurde in der Philosophie eigens eine „Metaethik“ entwickelt, die „Begründungs- und Rechtfertigungsmethoden moralischer Urteile“ (19, S. 10) zum Gegenstand hat. Betont werden muss aber, dass es nur eine bestimmte Denkrichtung in der Philosophie ist, in der eine philosophische Ethik als formal-technische Aufgabe begriffen wird. Wir werden auf andere philosophische Strömungen zu sprechen kommen, die die Aufgabe der Philosophie in der Ethik völlig anders bestimmen.

Welche Regeln sind Regeln von Moral und Ethik?

Wir hatten oben gesagt, dass ein Handeln dann moralisch ist, wenn es sich an in einer Gemeinschaft geteilten Auffassungen orientiert und dass Ethik die Auseinandersetzung mit solchen Auffassungen in Gedanken, Gesprächen und Texten ist. Doch sind Moral und Ethik zuständig für jede Art von gesellschaftlicher Regelung? Offenbar gibt es eine Vielzahl von Regelungen, die nicht moralisch-ethischer Natur sind: Höflichkeitsregeln (man gibt zur Begrüßung die rechte Hand), stilistische Regeln (z.B. in welchen Farben ein Haus bemalt sein darf), technische Regeln (z.B. welche Wattzahlen in einer Lampe erlaubt sind), Spielregeln (z.B. Abseits im Fußball) gelten nicht als moralische Regeln. Wer gegen solche Regeln verstößt, handelt nicht unmoralisch. Er handelt unhöflich, geschmacklos, unklug oder inkorrekt. Was also ist es, was eine Regel zu einer Regel der Moral macht? Wir hatten bisher davon gesprochen, dass ein Handeln moralisch ist, wenn es sich an bestimmten Auffassungen orientiert, nämlich an solchen davon, was gut und gerecht ist. Was unterscheidet nun aber Auffassungen davon, was gut und gerecht ist von etwa solchen darüber, was höflich, was

schön, was korrekt ist? Einige Ethiker und Moralphilosophen meinen, dass ein Handeln nur dann moralisch ist, wenn es sich letztlich an unbedingten, nicht mehr hinterfragbaren Prinzipien und „obersten Normen“ (19, S. 12) orientiert. Daran ist richtig, dass wir für gewöhnlich unsere Auffassungen davon, was gut und gerecht ist, nicht so leicht zur Disposition stellen wie eine Höflichkeits-, Mode- oder Abseitsregel. Andererseits ist uns durchaus bewusst, dass andere Menschen mit anderen Erfahrungen, oder auch anderen kulturellen Hintergründen, andere Auffassungen davon haben können, was in einer bestimmten Situation gut und gerecht ist. Jemand, der sich für den Statthalter des absolut Guten und absolut Gerechten hält, läuft Gefahr, zum Fanatiker zu werden. In Fragen der Moral geht es also um einen Ausgleich zwischen zwei starken Motiven: Auf der einen Seite sind unsere moralischen Auffassungen so beschaffen, dass wir an ihnen unbedingt festhalten wollen, auf der anderen Seite erfahren und wissen wir, dass auch – und gerade! – in moralischen Fragen sich gewichtige und konfliktträchtige Unterschiede zwischen den Auffassungen zeigen können. Dieser Zusammenhang von Unbedingtheit einerseits und Verschiedenheit andererseits ist ein zentraler Gegenstand moraltheoretischer Überlegungen. Er wird in der Ethik unter dem Titel ’Relativismus’ verhandelt. Wir kommen dazu in Abschnitt 1.6.

Der Zusammenhang von Moral, Ethik und Recht

Eine andere Reaktion auf diese Problematik ist die Einführung von Recht. Was ist Recht? Und wie verhält es sich zu Moral und Ethik?

Kehren wir zur Klärung dieser Fragen wieder zurück zu den Schiffsbrüchigen. Wir können uns vorstellen, dass die Diskussionen zwischen Vertretern verschiedener Auffassungen sich hin und her bewegen: zeitweise setzten sich die einen mit ihrer Auffassung durch, zeitweise die anderen, zweitweise gab es Patt-Situationen, in denen ganz unklar ist, was gilt und wie zu handeln ist. Das wird als unbefriedigend und unpraktikabel empfunden, so dass die Forderung laut wird, man solle die Regeln verbindlich festlegen und diejenigen bestrafen, die sich nicht an sie halten. Eine solche Festlegung von Regeln können wir als den Akt der Einführung von Recht verstehen.

Was ist Recht?

Recht wird folgendermaßen definiert:

D

Definition 1.4: Recht

„Gesamtheit der staatlich festgelegten bzw. anerkannten Normen des menschlichen, besonders gesellschaftlichen Verhaltens; Gesamtheit der Gesetze und gesetzähnlichen Normen; Rechtsordnung“ (11)

Rechtspositivismus

Doch ebenso wie die Bestimmung des Begriffs Ethik wirft auch die Definition von Recht Fragen auf, über die sich die Gelehrten uneins sind. Es entsteht nämlich folgendes Problem: Bestimmt man Recht tatsächlich nur als die Menge der durch gesetzgebende Institutionen festgelegten und durch staatliche Organe durchgesetzten Normen, dann muss man auch z.B. die von einem Diktator erlassenen Gesetze als Recht bezeichnen. Recht ist dann eine wertneutrale Sammelbezeichnung für festgesetzte Regelungen, gleich wie sie zustande kommen, gleich wie sie begründet sind. Eine solche Auffassung wird in der Rechtslehre Rechtspositivismus genannt.

Dagegen argumentieren andere Rechtsgelehrte, dass Gesetze nicht automatisch als Recht gelten können. Wenn z.B. Gesetze erlassen werden, die bloß der Herrschaftssicherung der Machthaber dienen, die willkürliche Privilegien und Diskriminierungen festschreiben, die menschenverachtendes Verhalten dulden oder fordern, so handele es sich um ungerechte Gesetze und damit nicht um Recht. Ein Gesetz ist demnach nicht schon allein dadurch Recht, dass es besteht. Damit ein Gesetz Recht ist, muss es vielmehr höheren Normen der Gerechtigkeit folgen.

E

Exkurs 1.2: Abkehr vom Rechtspositivismus

Gustav Radbruch, Reichsjustizminister in der Weimarer Republik und einer der einflussreichsten Rechtsphilosophen des 20. Jahrhunderts, hat, unter Eindruck des "Dritten Reiches", auf besonders eindrückliche Weise eine Abkehr vom Rechtspositivismus gefordert:

„Vielfältig haben die Machthaber der zwölfjährigen Diktatur dem Unrecht, ja dem Verbrechen die Form des Gesetzes gegeben. Sogar der Anstaltsmord soll durch ein Gesetz untergründet gewesen sein, freilich in der monströsen Form eines unveröffentlichten Geheimgesetzes. Die überkommene Auffassung des Rechts, der seit Jahrzehnten unter deutschen Juristen unbestritten herrschende *Positivismus* und seine Lehre ’Gesetz ist Gesetz’, war gegenüber einem solchen Un-

> recht in der Form des Gesetzes wehrlos und machtlos; die Anhänger dieser Lehre waren genötigt, jedes noch so ungerechte Gesetz als Recht anzuerkennen. Die Rechtswissenschaft muss sich wieder auf die jahrtausendealte gemeinsame Weisheit der Antike, des christlichen Mittelalters und des Zeitalters der Aufklärung besinnen, daß es ein höheres Recht gebe als das Gesetz, ein Naturrecht, ein Gottesrecht, ein Vernunftrecht, kurz ein übergesetzliches Recht, an dem gemessen das Unrecht Unrecht bleibt, auch wenn es in die Form des Gesetzes gegossen ist“. (33, S. 291)

Rechtspositivisten haben ihre Position immer wieder damit begründet, dass das Recht von moralischen Fragen und ethischen Auseinandersetzungen frei gehalten werden müsse. Doch offensichtlich ist es notwendig, auch Kritik an Gesetzen zu ermöglichen. Es muss die Frage gestellt werden können, ob ein bestimmtes Gesetz gerecht ist oder nicht.

Das Verhältnis von Moral und Recht

Das bedeutet nicht, dass jeder Einzelne seiner privaten Moral folgen und nach Belieben Gesetze beachten dürfe oder auch nicht. Es bedeutet, dass wir alle in dem Bewusstsein mit unseren Gesetzen leben und handeln sollten, dass auch Gesetze moralischer Bewertung und ethischer Diskussion unterliegen. Dies gilt sowohl für die Formulierung von rechtlichen Normen, als auch für ihre Auslegung und Durchsetzung.

Moral und Recht dürfen nicht in einem Konkurrenzverhältnis verstanden werden. Es geht nicht darum, moralische Maßstabe an die Stelle von rechtlichen Normen oder rechtliche Normen an die Stelle von moralischen Maßstäben zu setzen. Dass Gesetze als Recht gelten können, wird vielmehr erst dadurch garantiert, dass sie im Rahmen ethischer Diskussion stehen; und dass gemeinschaftliche ethische Überzeugungen auch wirklich zur Geltung kommen, wird dadurch garantiert, dass sie in einem Rechtssystem ausdrücklich formuliert und tatsächlich durchgesetzt werden. Recht und Moral können sich im Idealfall also gegenseitig stützen. Voraussetzung dafür ist, dass in einer Gesellschaft freie, öffentliche Debatten geführt werden, in denen unterschiedliche Vorstellungen, was in einer Sache gut und gerecht ist, vorgebracht werden (Ethik). Solche Äußerungen dürfen nicht ohne triftigen Grund verhindert werden und müssen eine Chance haben, sich in der öffentlichen Auseinandersetzung zu behaupten und in die rechtlichen Regelungen einzugehen. Im Rahmen solcher Debatten können auch veränderte moralische Werte, neue Anforderungen und Bedürfnisse

zum Ausdruck kommen, so dass rechtliche Normen verändert oder weiter entwickelt werden.

Kontrollaufgabe 1.2: Grundrechte

Nennen Sie zwei Grundrechte, die in Demokratien auch dafür garantieren sollen, dass staatliches Handeln und Gesetze an ethische Maßstäbe gebunden bleibt.

K

1.4 Moral, Ethik und Recht im Beruf

Ethik und Beruf

Neben allgemeinen ethischen Auffassungen haben viele Gemeinschaften, etwa Religionsgemeinschaften und Berufsstände gruppenspezifische moralische Regeln, z.B. einen Berufs- oder Standesethos entwickelt:

"Der 'Eid des Hippokrates' verpflichtet den Arzt in Anwendung der allgemeinen moralischen Forderung, seinen Mitmenschen in der Not zu helfen, auf die ärztliche Tätigkeit dazu, nach besten Wissen und Gewissen für das körperliche Wohlergehen und die Gesundheit der ihm anvertrauten Patienten zu sorgen.

Das Ethos des Lehrers besteht in der Forderung, die Schüler über die angemessene Vermittlung bestimmter Wissensinhalte zu aufgeklärten, mündigen Menschen zu erziehen.

Das Ethos des Busfahrers liegt in der Verantwortung für seine Passagiere, die er ungefährdet an ihr Ziel zu bringen hat."(32, S. 35)

Exkurs 1.3: The European Code of Police Ethics

Viele Organisationen und Unternehmen geben sich einen ethischen Code, um das Verhalten ihrer Mitglieder zu regeln. 2001 hat der Europäische Rat eine Empfehlung unter dem Titel The European Code of Police Ethics mit 66 Punkten verfasst. Folgende generelle Prinzipien zu polizeilicher Intervention (Punkte 35-46) sind dort zu lesen (Übersetzung WK):

„35. Die Polizei, und alle polizeiliche Operationen, müssen jedermanns Recht zu Leben respektieren.

36. Die Polizei darf unter keinen Umständen Folter, unmenschliche

E

oder degradierende Behandlung oder Bestrafung zufügen, einleiten oder tolerieren.

37. Die Polizei darf Gewalt nur anwenden, wenn es absolut notwendig ist und nur in dem Maße, in dem sie erforderlich ist, um legitime Ziele zu erreichen.

38. Die Polizei muss sich stets der Gesetzmäßigkeiten ihrer beabsichtigten Aktionen versichern.

39. Polizeiliches Personal soll Befehle seiner Vorgesetzten sorgfältig ausführen, doch es soll auch verpflichtet sein, die Ausführung von Befehlen zu unterlassen, die offensichtlich illegal sind und es soll darüber Bericht geben, ohne Sanktion befürchten zu müssen.

40. Die Polizei soll ihre Aufgaben in fairer Weise erfüllen, insbesondere geleitet von den Prinzipien der Unparteilichkeit und Nicht-Diskriminierung.

41. Die Polizei soll das individuelle Recht auf Privatheit nur beeinträchtigen, wenn es absolut notwendig ist und nur, um ein legitimes Ziel zu erreichen.

42. Die Sammlung, Speicherung und der Gebrauch persönlicher Daten durch die Polizei soll in Übereinstimmung mit internationalen Datenschutzbestimmungen erfolgen und insbesondere nur in dem Maße erfolgen, wie es zur Erfüllung gesetzlicher, legitimer und besonderer Aufgaben erforderlich ist.

43. Die Polizei soll sich in ihren Aktivitäten stets der für jedermann bestehenden fundamentalen Rechte bewusst sein, wie die Freiheit der Gedanken, des Gewissens, der Religion, des Ausdrucks, der friedlichen Versammlung, der Freizügigkeit und des friedlichen Genusses von Eigentum.

44. Polizeiliches Personal soll integer und respektvoll gegenüber der Öffentlichkeit handeln und dabei besonders die Situation von Individuen, die zu gefährdeten Gruppen gehören, berücksichtigen.

45. Polizeiliches Personal soll sich während eines Einsatzes normaler-

weise in seinem polizeilichen Status und seiner beruflichen Identität ausweisen können.

46. Polizeiliches Personal soll sich allen Formen von Korruption innerhalb der Polizei widersetzen. Es soll Vorgesetzte und andere mit Korruption befasste Instanzen innerhalb der Polizei informieren." (29, S. 10f)

Das Wort Beruf bedeutete ursprünglich: „persönliche Berufung [...], die völlige Hingabe verlangt und dafür Erfüllung verspricht" (37, S. 50). Zwar denken viele heute, dass die Erwerbsarbeit mit solchen anspruchsvollen Erwartungen nichts mehr zu tun hat, aber gerade solche Berufe, die mit großem persönlichen Einsatz, Verantwortung oder auch Gefahren verbunden sind, werden auch heute meist auf Grund einer bestimmten inneren Einstellung gewählt. Feuerwehrmann, Entwicklungshelfer/in, Polizist/in, Lehrer/in, Ärztin oder Sozialarbeiter (um nur einige Beispiele zu nennen) wird man nicht, weil man einen Job sucht, sondern auf Grundlage von Lebensentscheidungen. Man braucht in der Ausbildung viel Ausdauer und muss sich einige Qualifikationsstufen erarbeiten. Eine Überzeugung, dass die mit dem Beruf verbundenen Aufgaben und Tätigkeiten grundsätzlich gut und gerecht sind, ist erforderlich – rein egoistische Motive reichen für solche Berufe nicht aus. Die Berufsentscheidung hat also in vielen Berufen tatsächlich mit moralischen Einstellungen zu tun.

Ethische Problemstellungen im Beruf

Eine Schwierigkeit im Berufsleben besteht in der Frage, wie sich die Wertvorstellungen, die in der Berufswahl entscheidend waren, in der konkreten Ausübungen des Berufes realisieren lassen – oder auch nicht. Frustration und Burn-out sind nicht selten Folgen davon, dass sich Erwartungen und Wirklichkeit in einem Beruf schlecht in Übereinstimmung bringen lassen.

In der Berufs- und Wirtschaftsethik werden folgende Punkte hervorgehoben, an denen sich ethische Fragen stellen:

Verantwortung und die Entpersonalisierung von Entscheidungen

Verantwortung zu übernehmen für das Unternehmen oder der Institution, für Mitarbeitern und Untergebene, für eine Aufgabe oder ein Projekt gehört zu den elementaren Voraussetzungen guten beruflichen Handelns. Für gewöhnlich kann Verantwortung nur einem Individuum zugeschrieben werden: jede und jeder einzeln muss Verantwortung übernehmen, damit eine Gruppe oder Institution als ganze verantwortlich agiert. Doch das einzelne Verantwortungssubjekt ist in vielen Berufsbereichen immer weni-

ger gefragt: „Immer häufiger werden Entscheidungen [...] von Gruppen getroffen und von Organisationen umgesetzt.“ (39, S. 302). Organisationen schreiben Abläufe vor, so dass der Einzelne darauf festgelegt wird, nur noch gegenüber den Vorschriften korrekt, nicht aber verantwortlich zu handeln.

Loyalität und moralische Verantwortung

Eine Systemlogik – in Wirtschaftsunternehmen die Logik des Marktes, in staatlichen Institutionen 'Sachzwänge' und Verfahrensvorschriften – setzt sich an die Stelle der Verantwortung des Individuums. Daraus entsteht ein ethisches Dilemma: Einerseits ist es für den Erfolg und das Funktionieren des Betriebes erforderlich, dass sich Mitarbeiter loyal und regelgerecht verhalten. Sich loyal und regelgerecht zu verhalten gehört selbst zum Ethos des Berufes. Andererseits stehen die Logik des Marktes, die 'Sachzwänge' und Verfahrensvorschriften indifferent (gleichgültig) gegenüber moralischen Aspekten ihrer Prozesse. Das verantwortliche Individuum findet sich im Beruf deshalb immer wieder in Situationen von Zerreißproben zwischen moralischer Verpflichtung und moralischen Ansprüchen der jeweiligen Situation.

Eine Reaktion auf dieses Dilemma kommt aus dem ordnungstheoretischen Ansatz der Wirtschaftsethik. Karl Homann schlägt vor, zwischen 'Spielzügen' und Spielregeln' zu unterscheiden. Während die einzelnen Aktionen eines Berufstätigen innerhalb der Logik und Vorschriften seines Arbeitsgebietes 'Spielzüge' darstellen, bilden diese Logik und Vorschriften die 'Spielregeln', die das Handeln leiten. Daraus leitet Homann einen ethisches Prinzip ab: „Es ist die Pflicht jedes Wirtschaftssubjekts zu versuchen, an einer Änderung der Spielregeln mitzuwirken.“ (24, S. 314) Tatsächlich kann man erwarten, dass sich Situationen von Zerreißproben entschärfen, wenn das handelnde Individuum Möglichkeiten sieht, die Regeln, nach denen es sich in seinem Beruf zu richten hat, mitzugestalten und zu verändern. Tritt beispielsweise immer wieder das Problem auf, dass durch konformes Handeln Menschen benachteiligt oder unnötig in Schwierigkeiten gebracht werden, dann sollte die Möglichkeit gegeben sein und die Anstrengung unternommen werden, die Form des Handelns, also seine Vorschriften und Regelungen, zu ändern. Dieses ethische Gebot betrifft jeden Berufstätigen. Am stärksten aber ist hier das Leitungspersonal gefordert: Gemäß einer „Führungsethik“ hat das Leitungspersonal „Anreizsysteme“ für moralisches Verhalten der Mitarbeiter zu schaffen und auch „Instanzen, bei denen [die Mitarbeiter] gegen amoralische Unternehmenspolitik appellieren können.“ Eine Voraussetzung dafür ist „Transparenz“, die „durch

offene Informationsstrukturen im Unternehmen und durch gegenläufige Informationsströme erreichen“ läßt. (39, S. 330f).

Recht und Moral im Beruf

Auch in der Wirtschafts- und Berufsethik wird herausgestellt, dass das positive Recht allein keinen ausreichenden Rahmen für ethisches Handeln bereitstellen kann. Für Wirtschaftsunternehmen wird festgestellt: „Handlungen im ökonomischen Kontext können zwar entsprechend der geltenden Gesetzeslage legal sein, aber trotzdem gegen moralische Prinzipien verstoßen, also illegitim sein.“ (39, S. 315). Gleiches gilt für nicht-wirtschaftliche Institutionen und Berufsfelder. Rechtliche Bestimmungen und Verfahrensvorschriften allein reichen nicht aus, um verantwortliches und moralisch legitimes Handeln zu gewährleisten. Ethische Diskussionen und die Formulierung, Weiterentwicklung und Überarbeitung von ethischen Leitlinien und Ethikkodizes werden darüberhinaus benötigt, um moralische Sensibilität und Verantwortung in Unternehmen und Institutionen zu kultivieren.

K

Kontrollaufgabe 1.3: Ethische Verantwortung

Nennen Sie vier Punkte aus dem *European Code of Police Ethics* (siehe Exkurs 1.3), an denen Ermessensspielräume bestehen und daher ethische Verantwortung in besonderer Weise zum Tragen kommt.

1.5 Ethische Theorien

Im Folgenden werden Sie nun drei Typen von Ethik kennenlernen: (1) Utilitarismus, (2) Deontologie und (3) kompetenz- und situationsbezogene Ethiken.

Utilitaristische Ethik

Der Name Utilitarismus leitet sich vom lateinischen Wort für Nutzen ab. Eine utilitaristische Ethik ist also eine nutzenorientierte Ethik. Die Orientierung am Nutzen bedeutet im Utilitarismus aber nicht, dass jeder nur egoistisch seine eigenen Vorteil zu suchen hätte. Utilitarismus beruht vielmehr auf der Idee des größten Nutzens für die größte Zahl. Was maximiert werden soll, ist nicht der Eigennutz, sondern die Summe des Wohlergehens in einer Gesellschaft.

E

Exkurs 1.4: Das ’great happiness’-Prinzip

„Das ’great happiness’-Prinzip (s. d.) findet sich schon bei BECCARIA, HUTCHESON, besonders aber bei dem systematischen Begründer

> des Utilitarismus (im engeren Sinne), J. BENTHAM. Zweck, Ziel des sittlichen Handelns ist die Maximierung der Glückseligkeit, das größtmögliche Glück der größtmöglichen Anzahl, 'the greatest happiness of the greatest number', 'the greatest possible quantity of happiness' (Introd. II, ch. 17, p. 234. Deontolog.. Traité de la législat. civile et penale, 1802). [...] Das Interesse der Gemeinschaft ist 'the sum of the interest of the several members who compose it' (l. c. p. 4 ff.).“ (Eintrag 'Utilitarismus' in: (12))

Eigennutz und Gesamtnutzen sind im Utilitarismus aber nicht leicht zu trennen und es kommt hier oftmals zu Missverständnissen. Denn tatsächlich hat der Utilitarismus das konkrete, einzelne Individuum im Blick: dessen Wohlergehen ist der Betrag, der in die Gesamtsumme des gesellschaftlichen Glücks eingeht. So kann es scheinen, als ob das Streben nach individuellem Glück zugleich das ethisch Gebotene wäre: 'Geht es mir besser, dann trage ich mehr zur Summe des Gesamtglücks bei, also ist diese Summe größer', so ist Mancher versucht zu denken. Doch die Steigerung des eigenen Wohlergehens geschieht oft auf Kosten des Wohlergehens und der Entfaltungsmöglichkeiten anderer. An dieser Stelle beginnen die Schwierigkeiten einer utilitaristischen Ethik. Um den ethischen Wert einer Handlung bestimmen zu können, müssten die Vor- und Nachteile für alle möglicherweise Betroffenen, auch die, die in Zukunft davon betroffen sein könnten, sorgfältig abgewogen werden. Das aber ist außerordentlich schwierig und gelingt nur so weit, wie sich die Folgen durch Erfahrung und Menschenkenntnis tatsächlich einschätzen lassen.

Der Utilitarismus ist eine Lehre, die sich im 18. Und 19. Jahrhundert in England entwickelte. Der Hintergrund dieser Lehre ist die Welt des kaufmännischen Bürgertums, in der man gewohnt war, Gewinn- und Verlustrechnungen aufzustellen. Entsprechend ist die utilitaristische Ethik eine Ethik, die auf einem Kalkül beruht: Man glaubt, berechnen zu können, was als Endsumme zu erwarten ist, wenn man die glücks- und die leidfördernde Konsequenzen einer Handlung miteinander verrechnet. Daraus spricht „eine Zuversicht, der wir heute, nach vielen gescheiterten Versuchen, auch nur für den Bereich der vergleichsweise leicht zu erfassenden wirtschaftlichen Güter ein gesellschaftliches Wohlfahrtsmaximum zu bestimmen, weitaus skeptischer gegenüberstehen“ (5, S. 199).

Trotzdem hat der Utilitarismus einige Plausibilität für sich. Wenn auf der Insel der Schiffsbrüchigen beispielsweise einer sagte, „lasst uns sehen, dass

sich die Situation für möglichst viele von uns möglichst verbessert“, dann könnte er damit durchaus auf Zustimmung stoßen. Das Problem des Utilitarismus zeigt sich, wenn das Kalkül zur Erhöhung des Gesamtwohlergehens radikal und über alle sonstigen Wertvorstellungen hinweg durchgesetzt wird. Warum soll man – nach diesem Kalkül – nicht Alte und Kranke ausstoßen, wenn die Mühe der Pflege größer scheint als das Wohlergehen, das sich damit noch erreichen lässt? Solche Probleme treten auf, wenn der Wert des Lebens nicht an sich als Wert gilt, sondern nur in Hinsicht auf einen Gesamtnutzen. Ebenso ist es schwierig, Fragen der Gerechtigkeit utilitaristisch zu behandeln: „Das Prinzip der Nutzenmaximierung sagt nichts über die Kriterien der Nutzenverteilung. Es lässt offen, in welchem Maße [und nach welchem Kriterium, WK.] der einzelne an dem 'Glück der größten Zahl' teilhaben soll: nach seinem moralischen Verdienst, nach der von ihm erbrachten Leistung, nach der subjektiven Anstrengung, die diese ihn gekostet hat, oder nach dem Prinzip der Gleichverteilung“ (5, S. 202).

Der Utilitarismus hat sich in Reaktion auf solche Probleme weiter entwickelt und ist heute in ein Bündel ethischer Theorien aufgefächert. In seiner jüngeren Ausprägung unterscheidet der Utilitarismus zwischen dem Primärprinzip der Nutzenmaximierung und Sekundärprinzipien, nämlich denen der alltäglichen moralischen Praxis. Normalerweise handeln und entscheiden wir demnach gemäß alltäglicher moralischer Regeln, das Nutzenprinzip dient lediglich dazu, solche moralischen Regeln auf ihren ethischen Wert hin zu prüfen.

Deontologische Ethik

Damit nähern sich utilitaristische Ethiktheorien einem anderen Ansatz an, der für gewöhnlich als Gegenentwurf beschrieben wird: dem der deontologischen Ethiken. Das Wort deontologisch kommt vom altgriechischen Wort *to deon*, was 'die Pflicht', 'das Schickliche' bedeutet. Deontologische Ethiken bezeichnet man deshalb auch als Pflichtenethiken.

Im Kern unterscheidet sich eine deontologische Ethiken von utilitaristischen Ethiken darin, dass sie moralische Gebote als in sich selbst verbindlich betrachten. Utilitaristen rechtfertigen moralische Regeln dadurch, dass sie zu etwas dienen (nämlich zur Steigerung des Gesamtnutzens). Anhänger der Deontologie behaupten dagegen, dass moralische Regeln nicht durch etwas anderes als durch eine Begründung im Moralsystem selbst gerechtfertigt werden dürfen. Sie sagen: Moralische Gebote sind in sich selbst verbindlich, nicht, weil sie zu etwas anderem gut oder nützlich sind. Anders gesagt: Nicht die Konsequenzen oder Ziele, die man durch moralisches Handeln

verfolgt, sind entscheidend, sondern das Handeln in seiner Beschaffenheit selbst. Demgemäß unterscheidet man begrifflich konsequenzialistische bzw. teleologische Ethiken (auf Konsequenzen bzw. Ziele (telos = Ziel) bezogene Ethiken) von deontologischen Ethiken, die als nicht-konsequenzialistisch und nicht-teleologisch gelten. Der Hauptvertreter einer deontologischen Ethik ist der Philosoph Immanuel Kant (1724-1804). Kant hat sich die Aufgabe gestellt, ein logisch durchdachtes ethisches System aufzubauen, in dem sich moralisches Handeln schlüssig rechtfertigen lässt. Den Kern dieses ethischen Systems bildet der berühmte kategorische Imperativ. 'Imperativ' bedeutet eine 'befehlende Formulierung' und ein 'kategorischer Imperativ' ist ein Befehlsausdruck, „welcher eine Handlung als für sich selbst, ohne Beziehung auf einen anderen Zweck, als objektiv notwendig vorstellte“ (23, S. 242).

D

Definition 1.5: Kategorischer Imerativ

„Der kategorische Imperativ ist also ein einziger und zwar dieser: *handle nur nach derjenigen Maxime, durch die du zugleich wollen kannst, daß sie ein allgemeines Gesetz werde*.“ (23, S. 421)

Eine Maxime ist ein Maßstab des Handelns. Der kategorische Imperativ sagt also nicht direkt etwas darüber aus, welches Handeln moralisch ist, sondern etwas darüber, wie der Maßstab beschaffen sein soll, nach dem zu handeln ist. Dabei ist der kategorische Imperativ so etwas wie ein Test: „Dieser Test prüft Maximen, d.h. subjektive Handlungsmaßstäbe, danach, ob sie damit vereinbar sind, daß andere Personen sich die gleichen Maximen zu eigen machen.“ (30, S. 21) Der kategorische Imperativ stellt in Kants System die oberste Maxime dar. Er ist ein Maßstab, an dem sich alle anderen Maßstäbe zu orientieren haben. Allerdings ist er nicht nur allgemein gültig, sondern seine einzige inhaltliche Forderung ist die nach vollständiger Verallgemeinerbarkeit von Handlungsregeln: Der kategorische Imperativ fordert, dass jede Person ihre Maxime darauf hin prüft, dass sie sie nicht nur für sich selbst oder für seinesgleichen gelten lassen will, sondern für jede und jeden anderen auch. Der kategorische Imperativ stellt uns also jeweils vor die Frage: Kann ich meine Handlungsrichtlinie auch noch dann als gut befinden, wenn ich mir vorstelle, dass alle danach handeln?

In Kants ethischem System ist eine Handlungsrichtlinie also dann ethisch gerechtfertigt, wenn sie zugleich als allgemeines Gesetz gelten könnte. Das bedeutet, dass dieses System unabhängig davon, um welche moralische

Frage es gerade geht, ein formales Kriterium für das ethisch Richtige bereitstellt: Ethisch gerechtfertigt ist eine Handlungsleitlinie dann, wenn sie vollständig verallgemeinerbar („universalisierbar“) ist. Dieser formale Charakter von Kants deontologischer Ethik erweist sich oftmals als Schwäche, wenn es um konkrete moralische Fragen geht.

E

Exkurs 1.5: Kant: Kategorischen Imperativ

„Wie stets wieder gegen Kant geltend gemacht wurde, reicht das formale Prinzip des kategorischen Imperativs [...] zur Ableitung inhaltlich bestimmter moralischer Prinzipien nicht aus. [...] Falls ich etwa materiell in so guten Verhältnissen lebe, daß ich auf die Hilfeleistung anderer nicht angewiesen bin, würde ich es mir diesem Kriterium zufolge durchaus zum Prinzip machen können, anderen in einer Notlage niemals beizustehen, da ich ja durchaus wollen kann, daß diese meine Maxime allgemein akzeptiert wird. Die bloße Verallgemeinerbarkeit meiner Maxime kann also keine hinreichende, sondern allenfalls eine notwendige Bedingung ihrer moralischen Gültigkeit sein; das heißt, alle Maximen, die als Pflichterfüllung gelten wollen, müssen dieses Kriterium erfüllen, aber daß sie es erfüllen, reicht nicht aus, um sie zu Pflichten zu machen. Kant scheint diese Unzulänglichkeit durchaus gesehen zu haben. Er hat nicht nur den kategorischen Imperativ in dessen späterer, abweichenden Formulierung ansatzweise inhaltlich eingegrenzt, sondern ihm darüber hinaus – ungeachtet seines formalistischen Programms – in den Diskussionen einzelner Beispielfälle inhaltliche Normen an die Seite gestellt wie etwa die, seine Talente auszubilden und sich in seinem Handeln mit der objektiven Zweckmäßigkeit der Natur in Einklang zu setzen.“ (5, S. 235)

kompetenz- und situationsbezogene Ethiken

Ein dritter Typ von Ethik unterscheidet sich von den beiden bisher besprochenen utilitaristischen und deontologischen Ansätzen dadurch, dass er nicht voraussetzt, dass sich moralische Fragen einem einzigen logischen oder berechenbaren System fügen. Ethische Konzeptionen von diesem dritten Typ "bestreiten [...] gerade, dass es überhaupt möglich und sinnvoll ist, die Gesamtheit unserer berücksichtigungswerten moralischen Intuitionen und Argumente auf *einen* Nenner zu bringen, sie durch ein einziges übersichtlich konstruiertes Gedankenmodell zu fassen und an einem einzigen Moralprinzip zu orientieren."(40, S. 191)

Ein Problem mit ethischen Systemen besteht darin, dass sie in Bezug auf konkrete Fragen oft zu einander widersprechenden Schlussfolgerungen kommen. Für viele Probleme in der Medizin-, Bio-, Sozial- und Medienethik entsteht dadurch die Situation, dass die Expertenmeinungen auseinandergehen und dass komplexe moralische Fragen äls unvereinbare Alternativen dargestellt"werden (3, S. 192). Praktikern, die "konkrete Hilfe zur moralischen Orientierung seitens der Ethik suchen"(ebd.), ist damit kaum geholfen.

Eine Antwort auf diese Problematik könnte lauten: Die Idee, für moralische Probleme Entscheidungen aus logische Ableitungen oder Rechenkalkülen zu erhalten, ist an sich verfehlt. Es ist eine falsche Erwartung, dass sich Probleme komplexer Handlungssituationen, deren jede ja auch einzigartig ist, nach einem einheitlichen Schema, in einem einheitlichen System lösen lassen.

Diese Antwort verbindet ethische Ansätze miteinander, die sich als *Kompetenz- und situationsbezogene Ethiken* bezeichnen lassen.

D

Definition 1.6: Kompetenz- und situationsbezogenen Ethiken

Kompetenz- und situationsbezogenen Ethiken sind dadurch charakterisiert, dass sie als Voraussetzung für moralisches Handeln eine Kompetenz (eine gut entwickelte Fähigkeit) ansehen und dass sie diese Fähigkeit als eine Fähigkeit verstehen, situationsbezogen im moralischen Sinne richtig zu handeln.

Während utilitaristische Ansätze auf den angelsächsischen Empirismus und deontologische Ansätze auf den deutschen Idealismus zurückgehen, haben kompetenz- und situationsbezogene Ethiken ihren Ursprung in der antiken Philosophie, insbesondere in der Philosophie des Aristoteles.

Tugendethik

Die Ethik des Aristoteles wird als eine Tugendethik verstanden. Tugenden sind Eigenschaften von Menschen, nicht von Handlungen. Das bedeutet, dass diese Form von Ethik weniger darauf hin angelegt ist, Handlungen kritisch einzuschätzen, vielmehr richtet sie sich direkt an Menschen. Und zwar mit zwei Aufforderungen: Erstens, sollten wir so handeln, wie unter ähnlichen Umständen ein tugendhafter Mensch handeln würde. Zweitens sind wir aufgefordert, unsere Anlagen zur Tugend, die jeder Mensch in sich trägt, möglichst umfassend zu entfalten. Die Tugendethik zielt also

auf die Fähigkeit des Menschen, sich zu entwickeln und nach Besserem zu streben. In Bezug auf die Frage, was als Tugend angestrebt werden sollte, spricht Aristoteles von klassischen Werten wie Tapferkeit, Besonnenheit, Freigebigkeit, Sanftmut und Gerechtigkeit. Der eigentliche ethische Impuls kommt dadurch zustande, dass gemäß der Aristotelischen Ethik diese traditionellen Werte nicht einfach hingenommen werden, sondern im Sinne einer Lehre entwickelt werden, die die 'richtige Mitte' sucht. Diese sogenannte *Mesotes-Lehre* besagt, dass wir uns darum bemühen sollten, zum Beispiel in der Tugend der Tapferkeit die richtige Mitte zwischen dem Extrem des draufgängerischen Leichtsinns und dem Extrem der unbegründeten Furchtsamkeit zu finden. Dabei zielt diese Lehre „nun aber gerade nicht darauf ab, dass man einen möglichst leidenschaftslosen Zustand erreichen sollte, sondern dass man die Leidenschaft auf die richtige Weise haben soll" (34, S. 74).

Moderne kompetenz- und situationsbezogene Ethiken

Eine ganze Reihe von modernen Ethiken bauen auf dem Aristotelischen Erbe auf. Insbesondere der Gedanke, dass zu moralischem Verhalten auch kulturelle Voraussetzungen, gute Vorbilder, gute Erziehung und die Anleitung zur Fähigkeit, im moralischen Sinne klug zu handeln gehört, haben moderne Tugendethik, hermeneutische Ethik, Klugheitsethik, Kommunitarismus und einige Formen der sprachanalytischen Ethik gemeinsam. Alle diese Ethikansätze gehen davon aus, dass sich nicht logisch ableiten, berechnen oder sonstwie vorschreiben lässt, was in einer Situation moralisch richtig ist, sondern dass es in der Ethik um die Frage gehen müsse, wie man Menschen in die Lage versetzt, moralisch orientiert zu handeln.

E

Exkurs 1.6: Kompetenz- und situationsbezogenen Ethiken

Der US-amerikanische Philosoph und Pädagoge John Dewey hat in seinem Buch „Theory of the Moral Life" von 1908 eine Sichtweise, die für kompetenz- und situationsbezogenen Ethiken typisch ist, anschaulich formuliert:

„Ein moralisches Prinzip, wie etwa das der Keuschheit, das der Gerechtigkeit, das der Goldenen Regel, gibt dem Handelnden eine Grundlage, ein spezielles Problem, das auftaucht, vor sich zu bringen und zu untersuchen. Es stellt ihm mögliche Aspekte einer Handlung vor Augen; es warnt ihn davor, eine zu kurz greifende oder einseitige Sicht bezüglich der Handlung einzunehmen. Es ökonomisiert seinen Denkprozeß, indem es ihn mit den Hauptaspekten ausstattet, hinsichtlich

derer die Auswirkungen seiner Wünsche und Absichten zu bedenken sind; es leitet ihn in seinem Denken an, indem es ihn auf wichtige Erwägungen stößt, die ihm nicht entgehen sollten. Ein moralisches Prinzip ist also nicht ein Befehl, in einer bestimmten vorgegebenen Weise zu handeln oder darauf zu verzichten; es ist ein Werkzeug um eine spezielle Situation in ihrer Gesamtheit, und nicht nur durch die Regel als solche, zu analysieren." (9, S. 141; Übersetzung WK)

1.6 Ethischer Relativismus

Wir machen alltäglich die Erfahrung, dass es sehr unterschiedliche Auffassungen darüber gibt, was in einer Frage moralisch richtig und moralisch verwerflich ist. Teilweise unterscheiden sich die Auffassungen anderer von unseren eigenen sogar so tiefreichend, dass sie nicht nur in einer Sache zu anderen Schlüssen führen, sondern dass ihnen offenbar ganz andere Annahmen, was wichtig und was wertvoll ist, zu Grunde liegen. Es gibt offenbar verschiedene Systeme moralischer Werte und Richtlinien, in denen sich unterschiedliche Menschen orientieren.

Einige Ansätze der philosophischen Ethik bestehen in dem Versuch, diese Vielfalt einem rationalen oder logischen Kalkül zu unterwerfen. Sie zielen darauf, Formen des ethischen Argumentierens, Begründens und Ableitens zu entwickeln, so dass sich wohl begründete von schlecht begründeten moralischen Urteilen unterscheiden lassen. Dagegen ist aber eingewandt worden, dass rein formale Richtigkeit die Gültigkeit eines moralischen Urteils nicht sicherstellt. Wenn solche ethischen Begründungen aber inhaltliche Komponenten enthalten, so sind sie selbst schon bestimmten moralischen Voraussetzungen und Wertsystemen geschuldet. Jedes moralische Urteil steht immer schon unter bestimmten Voraussetzungen, ist immer schon bezogen – „relativ" – zu bestimmten moralischen Werten. Entsprechend lautet die Grundthese des ethischen Relativismus:

D

Definition 1.7: Ethische Relativismus

Der ethische Relativismus ist durch folgende Überzeugung definiert: „Es gibt keine allgemeinverbindlichen Urteile darüber, was moralisch richtig oder falsch ist." (19, S. 24).

Allerdings lässt sich diese Grundthese in sehr verschiedenen Weisen verstehen. Es ist zu unterscheiden zwischen moralischem Subjektivismus,

ethischem Kulturrelativismus und dem Problem multikultureller Gesellschaften. Der moralische Subjektivismus geht davon aus, dass ethische Fragen in die Privatsphäre des je einzelnen Subjekts fallen. Demnach hätte jeder Einzelne seine eigenen moralischen Werte und Richtlinien, an denen er sich orientiert. Die Unmöglichkeit allgemeinverbindlicher Urteile wird hier so interpretiert, dass über das hinaus, wie der Einzelne seine Überzeugungen gewinnt und sein Handeln ausrichtet, keine verbindlichen Richtlinien geben kann. Diese Position des moralischen Subjektivismus sieht sich mit zwei Einwänden konfrontiert:

Moralischer Subjektivismus

1. Die moralischen Richtlinien des Einzelnen entstehen stets in Übernahme und in Auseinandersetzung mit Werten, die in Familie, Schule, Freundeskreis, Beruf vermittelt werden. Kein Mensch entwickelt sich völlig isoliert von gesellschaftlichen Verbünden, die menschliche Entwicklung erfolgt als Sozialisation. Daher ist jede moralische Selbstverständigung, auch die Zurückweisung und Abgrenzung von den Werten der Eltern zum Beispiel, stets eine Antwort auf bestimmte, in einer Gesellschaft vermittelte moralische Richtlinien, keine Neuschöpfung nach bloß eigener Maßgabe.

2. Da moralische Richtlinien in weiten Bereichen das Verhältnis und Verhalten zu anderen betreffen, stehen sie in ständigem Kontakt und Konfrontation mit den Richtlinien derer, die von diesem Verhalten betroffen sind. Ethische Auseinandersetzung und Abstimmung mit anderen, und damit eine Reflexion, die die eigene Privatsphäre überschreitet, läßt sich also gar nicht vermeiden.

K

Kontrollaufgabe 1.4: Racial Profiling

Von 'Racial Profiling' wird gesprochen, wenn Personal von Polizei, Zoll oder anderen Sicherheitsdiensten Menschen einer bestimmten 'Rasse', Ethnie, Kultur oder Religion pauschal kritischer inspiziert als andere Menschen. Ordnen Sie die folgenden vier Aussagen den vier Ethiktypen Utilitarismus, Deontologie, kompetenz- und situationsbezogene Ethiken und moralischem Subjektivismus zu.

1. „Da tickt jeder Beamte anders. Wen er sich bei der Kontrolle herausgreift, muss jeder selbst entscheiden."

2. „'Racial Profiling' ist nicht effektiv. Die Belastungen für die Betroffenen und der Schaden für das Vertrauensverhältnis zwischen bestimmten Bevölkerungsgruppen und Sicherheitspersonal ist viel größer als der Sicherheitsgewinn, der sich durch Kontrollen auf Grund von pauschalem Verdacht erreichen läßt."

3. „Es ist für mich ein hoher Wert, Menschen vorurteilsfrei gegenüber zu treten, unabhängig davon, welchen ersten Eindruck ich habe. In vielen Momenten muss ich aber spontan entscheiden. Es wäre gut, noch besser darin geschult zu werden, Vorurteile von begründeten Verdachtsmomenten zu unterscheiden."

4. „Aus dem Prinzip der Gleichheit und dem Verbot jeglicher Diskriminierung, wie sie auch im Grundgesetz und im internationalen Recht verankert sind, leitet sich ab, dass 'Racial Profiling' ethisch nicht zu befürworten ist."

ethischer Kulturrelativismus

Vom moralischen Subjektivismus ist der ethische Kulturrelativismus zu unterscheiden. 'Kulturrelativismus' bedeutet, dass unterschiedliche Kulturen unterschiedliche Ideen- und Handlungssysteme entwickeln, die sich nicht auf eine einheitliche Grundstruktur von logischer oder natürlicher Ordnung zurückführen lassen. 'Ethischer Kulturrelativismus' bedeutet, dass auch die moralischen Werte in unterschiedlichen Kulturen je eigene Ordnungen bilden, die die Richtlinien für das Handeln in den jeweiligen Kulturen bilden. Es gibt demnach keine für alle Menschen gleichermaßen gültige – „universale" – moralische Prinzipien, die moralische Prinzipien hängen von der jeweiligen Kultur ab.

Die beiden Einwände, die gegen den moralischen Subjektivismus vorge-

bracht werden, betreffen den ethischen Kulturrelativismus offenbar nicht. Der ethische Kulturrelativismus geht ja gerade davon aus, dass moralische Richtlinien ein gemeinschaftlich geteiltes Gut sind, das sich im Zusammenleben entwickelt und darin Gültigkeit gewinnt.

Gegen den ethischen Kulturrelativismus wird häufig der Einwand erhoben, dass er eine allgemeingültige Aussage voraussetze, die er gerade negiere. So sei die Forderung, andere Kulturen seien in ihren anderen Maßstäben zu tolerieren, „selbst eine universal gültige Norm, aber die Existenz solcher universeller Normen wird von den Relativisten ja gerade bestritten." (35, S. 482) Es ist allerdings fraglich, ob sich Kulturrelativisten tatsächlich auf universale Allgemeinaussagen festlegen lassen. Den meisten Kulturrelativisten geht es weniger um die (tatsächlich universalistische und problematische) Behauptung, alle Kulturen seien prinzipiell verschieden, sondern darum, einzelne Handlungs- und Sichtweisen im Zusammenhang mit der Kultur zu verstehen, in der sie stehen.

E

Exkurs 1.7: Interpretation von Handlung im kulturellen Zusammenhang

Ein Beispiel, wie unterschiedlich eine Handlung zu interpretieren sein kann, wenn man sie in ihrem kulturellen Zusammenhang betrachtet, gibt der amerikanische Philosoph Richard B. Brandt in seinem Text „Drei Formen des Relativismus" von 1961:

„Die Römer waren der festen Überzeugung, es sei verwerflich, seinen Vater zu ermorden und sahen die furchtbarsten Strafen für den vor, der dieses Kapitalverbrechen verübte. Die Römer würden sicher erklärt haben: „Es ist falsch, seinen Vater zu töten." Andererseits gab es primitive Stämme, bei denen es zu den Sohnespflichten gehörte, seinen Vater zu töten. Angenommen, wir sprächen mit einem Südseebewohner, in dessen Stamm es üblich ist, daß der Sohn den Vater an dessen 60. Geburtstag lebendig begräbt, und zwar ohne Rücksicht auf dessen Gesundheitszustand. Vermutlich würde dieser Südseebewohner sagen: „Es ist richtig, seinen Vater zu töten." Nun stellt sich die Frage, ob es sich hier um einen Unterschied in den grundlegenden moralischen Axiomen handelt. Möglicherweise, aber nicht unbedingt. Gewiß wird Vatertötung gegensätzlich beurteilt. Aber hat die Tötungshandlung dieselbe Bedeutung für beide? Nicht in jeder Beziehung. Der Südseebewohner mag etwa der Meinung sein, der

Körper seines Vaters werde im nächsten Leben dieselbe Gestalt behalten wie im Zeitpunkt des Todes. Unter diesen Umständen erscheint es ratsam, aus dem Leben zu scheiden, bevor der Körper von Schwäche befallen wird. Dem Römer dagegen mag diese Überzeugung über das Jenseits fehlen; er glaubt vielleicht überhaupt nicht an ein Leben nach dem Tode. So redet der Südseebewohner über das Lebendigbegrabenwerden seines Vaters, der in der nächsten Welt in einer bestimmten körperlichen Verfassung existieren wird, der Römer aber nicht. Hier schiene es mir nur verwirrend zu sagen, zwischen dem Römer und dem Südseebewohner bestünde ein Gegensatz in grundlegenden moralischen Axiomen. Denn die moralischen Bewertungen der beiden beziehen sich nicht eigentlich auf dieselbe Handlung, das heißt auf eine Handlung, die für beide genau die gleiche Bedeutung hat.“ (7, S. 45)

kulturelle Vielheit

Der ethische Kulturrelativismus ist da von besonderer Bedeutung, aber stößt auch an Grenzen, wo es um das Zusammenleben von Menschen unterschiedlicher Kulturen geht. Es stellt sich hier die Frage, inwieweit eine Gesellschaftsordnung eine Ausrichtung des Handelns an kulturell geprägte Handlungsrichtlinien ermöglichen kann bzw. muss. Eine Extremposition wäre hier ein Relativismus, der jede Handlungsweise, sofern sie sich auf eine kulturelle Tradition berufen kann, als prinzipiell legitim ansehen würde. Der extreme Gegenpol bestünde in der Auffassung, dass ein bestimmtes Moralsystem, etwa weil es das „rationalste“, das „fortschrittlichste“ oder das schlicht das „hier etablierte“ sei, bei allen Mitgliedern einer Gesellschaftsordnung durchzusetzen sei.

Als Beispiel für einen differenzierten Zugang zu ethischen und rechtlichen Fragen unter Bedingungen kultureller Vielheit lesen Sie die im Folgenden abgedruckten Ausschnitte aus einem Artikel des ehemaligen Verfassungsrichters Dieter Grimm und beantworten Sie die Fragen zu diesem Text.

E

Exkurs 1.8: Ethischen und rechtlichen Fragen unter Bedingungen kultureller Vielheit

„[Das] Grundgesetz [ist] eine Verfassung, die sich zu Toleranz, auch zu Toleranz gegenüber kultureller Andersartigkeit, bekennt. Zu seinen maßgeblichen Prinzipien gehören die in der Menschenwürde wurzelnde Gleichheit aller, die freie Entfaltung der Persönlichkeit, die

Glaubens- und Gewissensfreiheit, die Freiheit der Meinung und der Kunst, die Freiheit, sich zu versammeln und Vereinigungen zu bilden. Kurz: Meinungsunterschiede, Pluralität von Religionen und Weltanschauungen, kulturelle Vielfalt sind nach der Verfassung legitim; Andersartigkeit muss im Prinzip ertragen werden. Jeder kann seine Lebensform wählen und seine Auffassung vertreten. Jeder kann auch andere Auffassungen und Lebensformen ablehnen, nicht aber ihr Existenzrecht verletzen. Der Staat hat die Freiheit aller zu garantieren und darf für keinen Partei ergreifen. [...]

Das heißt aber nicht, dass der Einwanderer [...] der einheimischen Bevölkerung seine kulturellen Eigenheiten aufnötigen darf. Ebenso wenig heißt es, dass er auf die Überzeugungen und Gewohnheiten der einheimischen Bevölkerung keine Rücksicht nehmen muss. Das Grundgesetz ist nicht wertneutral, sondern auf den Wert der Menschenwürde und die daraus folgenden Grundsätze individueller Selbstbestimmung und gleicher Freiheit gegründet. [...]

Das Grundgesetz geht davon aus, dass sich die Freiheit aller nur garantieren lässt, wenn keine einzelne Freiheit unbegrenzt ist. Da jede Freiheit, auch die religiöse, in Konflikt mit anderen Freiheiten oder derselben Freiheit anderer geraten kann, sind gesetzliche Beschränkungen zur Verhütung von Freiheitsmissbrauch und zur Wahrung wichtiger Gemeinschaftsgüter nötig und zulässig. Sie gelten grundsätzlich für alle, die sich auf das Gebiet der Bundesrepublik begeben, ungeachtet ihrer kulturellen Herkunft. Die Frage ist nur, ob bei einem Konflikt zwischen einer fremden Kultur und der deutschen Rechtsordnung die Verfassung Ausnahmen von Freiheitsbeschränkungen zulässt oder gar gebietet. Es geht also um das Verhältnis von Einheit und Differenz, Gleichheit und Dispens, das bei jedem Zusammentreffen unterschiedlicher Kulturen nach Klärung verlangt. [...]

Im Bereich der Ausnahmen von allgemein geltenden und an sich wohl begründeten Regelungen zugunsten kultureller Minderheiten ist der Toleranzspielraum größer, als gewöhnlich angenommen. So sollte niemand an der Erfüllung religiöser Pflichten nur deswegen gehindert werden, weil sich die einheimische Bevölkerung durch die Fremdartigkeit des Verhaltens irritiert zeigt oder allein an dem Vorhandensein von Ausnahmen Anstoß nimmt. [...]

Solche Ausnahmen sind auch keineswegs eine Neuigkeit. Die Rechtsordnung ist vielmehr voll von Ausnahmen zugunsten bestimmter Gruppen: Jugendliche sind vom allgemeinen Strafrecht ausgenommen. Arbeitnehmer, die dem Betriebsrat angehören, fallen nicht unter das allgemeine Kündigungsrecht. Beamte werden von der gesetzlichen Altersversicherung ausgenommen. Arme Menschen sind von der Bezahlung der Rundfunkgebühr befreit, Priester von der Wehrpflicht. Der gesellschaftliche Zusammenhalt oder die Rechtstreue der Bevölkerung haben darunter nicht gelitten. Es bedarf der Einsicht, dass kulturelle Unterschiede ebenso gute Gründe für Befreiungen sein können. [...]

Was für Ausnahmen von allgemeinen Verboten gilt, muss jedoch nicht für Ausnahmen von allgemeinen Erlaubnissen gelten. Dort ist der Spielraum für Toleranz in der Regel geringer. Jede Begrenzung der allgemeinen Freiheitssphäre zugunsten der kulturellen Identität einer Minderheit kann für das einzelne Mitglied dieser Minderheit einen erheblichen Freiheitspreis haben. In den USA stellte sich die Frage, ob die Mitglieder der religiösen Gruppe der Amish ihre Kinder in den beiden letzten Jahren der Schulpflicht in eine öffentliche Schule schicken müssen oder ob sie davon zu entbinden seien. Nach Ansicht der Amish wurden ihre Kinder in öffentlichen Schulen zu Werthaltungen und Lebensweisen erzogen, die den eigenen krass widersprechen. Der Supreme Court erkannte dieses Argument an, weil die Durchsetzung der allgemeinen Schulpflicht für die Gruppe identitätsvernichtendes Gewicht hätte. In Deutschland sind Schulpflichtfälle anders entschieden worden. Allerdings wäre wohl auch die US-Entscheidung anders ausgefallen, hätten nicht die Eltern *gegen*, sondern Amish-Schüler *für* die Ausbildung in einer öffentlichen Schule gestritten.

Das gilt erst recht, wollte eine Minderheit zur Wahrung ihrer kulturellen Identität ihren Mitgliedern Verhaltensweisen verbieten oder aufnötigen, die gerade den fundamentalen Freiheits- und Gleichheitsverbürgungen der einheimischen Rechtsordnung entgegenstehen. Die Gesellschaft ist nicht gezwungen, zur Anerkennung fremder kultureller Identität die eigene Identität aufzugeben. Im Bereich der Gleichberechtigung werden sich dafür besonders viele Beispiele finden. Die Zwangsverheiratung von Mädchen, rituelle Verstümmelungen, Ausschluss von höherer Bildung, aber auch entehrende Strafen oder

Meinungs- und Informationsverbote dürfen daher selbst dann nicht toleriert werden, wenn sie religiöse oder sonstige kulturelle Wurzeln haben. Nicht alle Kulturkonflikte lassen sich harmonisch lösen. In bestimmten Kernbereichen bleibt nur die Alternative von Anpassung oder Wegzug.“ (14)

1.7 Technikethik

Neue ethische Herausforderungen durch Technik

Bisher haben wir hauptsächlich ethische Fragen in den Blick genommen, wie sie sich im unmittelbaren Umgang der Menschen miteinander stellen: Was ist gut und gerecht in der Verteilung von Gütern, in der Erfüllung beruflicher Aufgaben, im Verhältnis zu Hilfs- und Schutzbedürftigen, in der Beziehung zu kulturell Andersdenkenden. Eine neue Dimension ethischer Problemstellungen tritt hervor, wenn in einer Gemeinschaft Technik zum Einsatz kommt. Ein Angelhaken, ein hochseetaugliches Boot oder ein Pflug ist nicht nur ein Gut, für das sich die Frage stellt, wie die Teilhabe an diesem Gut in einer Gemeinschaft moralisch richtig zu regeln ist, sondern es ist zugleich ein Potenzial: Ein solches Instrument verschafft denjenigen, die darüber verfügen und damit umzugehen wissen, eine Produktivität und Handlungsspielräume, über die die anderen nicht verfügen. Dies wäre unproblematisch, wenn der Vorteil, der durch Technik erlangt wird, sich stets und gleichmäßig als Vorteil für alle auswirken würde. Doch die technischen Mittel, die die einen einsetzen, können sich auch zum Nachteil für andere auswirken: Neue Fortbewegungsmittel, chemische Stoffe, Herstellungstechniken stellen zwar häufig Verbesserungen innerhalb eines technischen Aufgabenbereichs dar, bedeuten aber zugleich neue Gefahren für Betroffene, die nicht unbedingt zugleich – oder in gleichem Maße – davon profitieren. Mit neuen technischen Anlagen können zwar neue Produkte hergestellt und auf den Markt gebracht werden, sie können aber zugleich – etwa durch Verschmutzung von Luft, Böden und Wasser, durch Lärm und Gesundheitsgefährdung, durch Verbrauch an Land und Ressourcen, durch Zerstörung von natürlichen Lebensräumen andere in ihren Handlungsmöglichkeiten einschränken, ihnen sogar die Lebensgrundlage entziehen.

Technik ist zu einem zentralen Thema aktueller Ethik geworden, weil die mit ihr verbundene Steigerung von Möglichkeiten und Effekten auch die Konflikte verschärft, die zwischen den Handlungsweisen verschiedener Akteure entstehen können. Vor- und Nachteile, Wirkungen, Neben- und Langzeitwirkungen müssen hinsichtlich der Frage, was gut und gerecht ist, immer wieder neu verhandelt und ausbalanciert werden.

Technik wird also zu einem ethischen Problem vor allem dann, wenn Technik neue Situationen schafft und die Voraussetzungen für Handeln und Leben verändert. Entsprechend wird der Technikbegriff der Technikethik so definiert, dass er in erster Linie auf dieses Veränderungspotenzial von Technik zielt.

D

Definition 1.8: Der Technikbegriff der Technikethik

Der Technikbegriff der Technikethik: „Der dabei zugrunde gelegte Technikbegriff bezieht sich in der Regel auf neue Techniken, Technologien oder Großtechnologien, die entweder moralische Fragen aufwerfen, zu deren Beantwortung die gesellschaftlichen Üblichkeiten nicht hinreichen, oder die zu moralischen Konflikten führen.“ (15, S. 284)

Antworten auf Einwände gegen Technikethik

Technikethik spielt in der dynamischen technischen Entwicklung moderner Gesellschaften eine wachsende Rolle. Jedoch ist in den diesbezüglichen Debatten nicht unumstritten, ob Technik überhaupt sinnvollerweise Gegenstand der Ethik sein kann. Es sind vier Annahmen, die den Sinn einer Technikethik in Frage stellen und gegen die sich das Unternehmen einer Technikethik behauten muss:

1. Ein Fortschrittsglaube, demgemäß alle Technik stets letztlich dem Menschen dient. Wäre dies zutreffend, wäre Technik an sich gut und gerecht und ethische Debatten über Technik erübrigten sich. Aus Sicht der Technikethik stellt sich eine solche Annahme als unhaltbar naiv und dogmatisch dar.

2. Eine generelle Technikfeindlichkeit, der gemäß alle Technik grundsätzlich von Übel ist. Auch hier erübrigte sich jegliche differenzierende Reflexion; allerdings aus ebenso wenig überzeugenden Gründen wie in Annahme (1).

3. Eine Sichtweise, die Technik als naturwüchsige, schicksalhafte Entwicklung betrachtet: Technik entwickelte sich gemäß dieser Annahme nach Gesetzmäßigkeiten, die unveränderlich und daher der Gestaltung entzogen sind. Eine gewisse Plausibilität erhält diese Sichtweise durch die Tatsache, dass technische Entwicklung insgesamt voranschreitet, ohne dass sie einem bestimmten Plan oder vorgegebenem Programm folgt. Allerdings ist der Schluss auf die Unveränderlich-

keit und Nichtgestaltbarkeit bestimmter technischer Entwicklungen aus Perspektive der Technikethik ein Fehlschluss. Auch Naturprodukte, die ohne menschliches Zutun entstanden sind, werden der Um- und Verarbeitung unterworfen. Wie könnte dann Technik, die ohne menschliche Gestaltung gar nicht entstünde, dem gestaltenden Zugriff entzogen sein?

4. Die These von der Neutralität der Technik: Technik ist gemäß dieser Annahme ein neutrales Mittel: ein Messer kann dazu dienen, Brot zu schneiden oder dazu, einen Menschen zu ermorden. Daher seien nicht die technische Mittel, sondern nur die Zwecke, für die die Technik eingesetzt werde, Gegenstand ethischer Fragen. Aus Perspektive der Technik-ethik verkennt diese Sicht allerdings, wie technische 'Mittel' auch unabhängig von ihren Zwecken Auswirkungen auf die Handlungsmöglichkeiten und Lebensbedingungen von Akteuren haben. Die scheinbare Plausibilität des Messerbeispiels kommt nur dadurch zustande, dass der moralisch richtig Umgang mit gefährlichen Gegenständen in Gesellschaften durch Erziehung und Sanktionen weitgehend gewährleistet wird. Es ist kein Zufall, dass es moralisch verwerflich erscheint, Kinder oder unberechenbare Personen mit gefährlichen Gegenständen auszustatten. Die scheinbare Neutralität von Mitteln erweist sich aus Perspektive der Technikethik als eine Neutralisierung schädlicher Potenziale, die gerade auf Moral und ethischer Reflexion beruht.

Zwei Schlüsselbegriffe der Technikethik sind Verträglichkeit und Verantwortung.

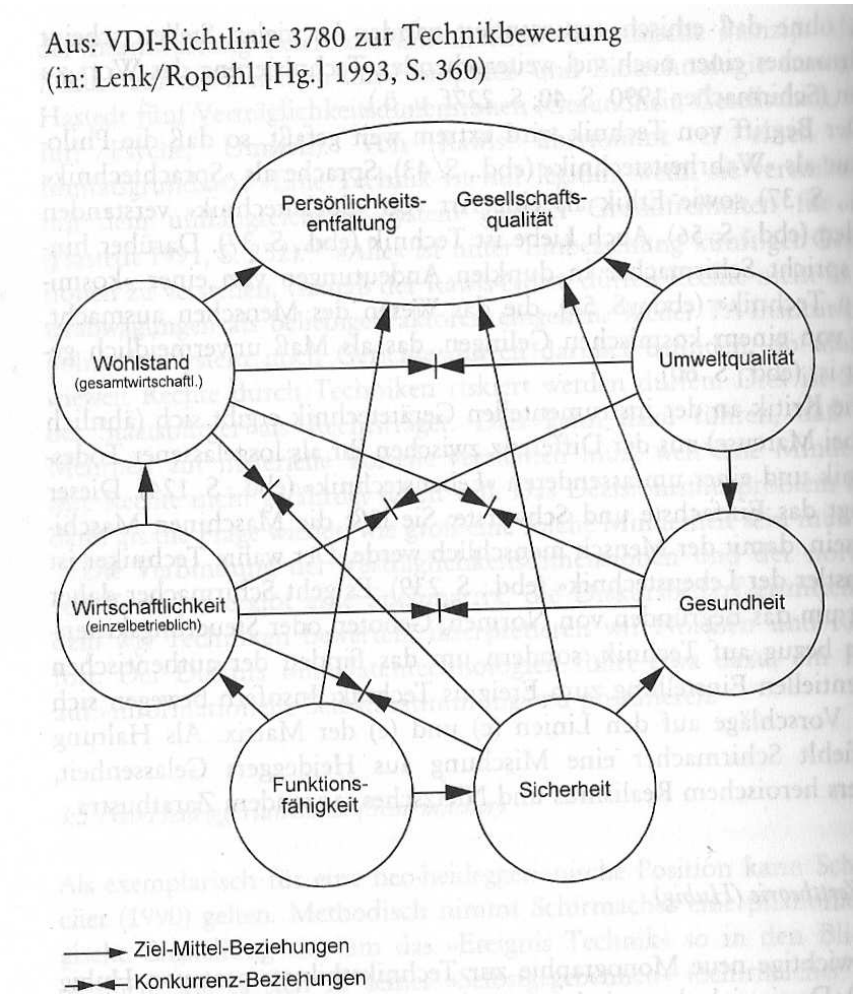
Verträglichkeit von Technik

Unter der Perspektive der Verträglichkeit ist neue Technik danach zu befragen, inwiefern sie „die Macht und das Wissen jedes Einzelnen vermehrt und ihm erlaubt, seine Kreativität zu betätigen, ohne damit notwendigerweise dem anderen diesen Spielraum zu verschließen.“ (21, S. 13f.)(Illich 1975, 13f.) Dabei lassen sich nach Hastedt fünf Dimensionen der „Auswirkungen und Voraussetzungen“ unterscheiden: Gesundheit, Gesellschaft, Kultur, Psyche, Umwelt. (16, S. 74ff.; 94ff.) Das bedeutet, dass hinsichtlich der Verträglichkeit neuer Technik neben manifesten Effekten auf Umwelt und Gesundheit auch schwierigerer zu erfassende Auswirkungen im Feld des psychischen Wohlergehens und Feld des kulturellen Entfaltung zu berücksichtigen sind. Es stellt sich in Hinblick auf Verträglichkeit von Technik nicht nur die Frage, welcher Einsatz welcher Technik moralisch richtig ist, sondern darüber

hinaus: wie wirkt sich dieser Einsatz auf die Lebensqualität der direkt und indirekt Betroffenen insgesamt aus.

Die Abbildung 1.1 zeigt einen Versuch des "Vereis deutscher Ingenieure"(VDI), einige der für Technik relevanten Richtwerte in ihren Beziehungen untereinander darzustellen.

Abb. 1.1: Aus: VDI-Richtlinie 3780 zur Technikbewertung



Technik und Verantwortung

Ein zweites Grundthema der Technikethik ist mit dem Begriff Verantwortung verknüpft. Verantwortung ist ein dialogischer Begriff: Man ist für etwas „vor oder gegenüber jemandem“ verantwortlich. Verantwortlich zu sein unterscheidet sich vom Rechenschaft abgeben in einem persönlichen Autoritätsverhältnis (gegenüber dem Vorgesetzten; dem Lehrer, den Eltern o.ä.) dadurch, dass nicht der Wille oder die Anweisung der Autorität maßgeblich sind, sondern Verantwortung stets nur „aufgrund bestimmter normativer Standards„ (40, S. 543) besteht. Verantwortung bezieht sich also darauf, was in ethischer Verhandlung als gut und gerecht bestimmt ist. Dabei kann Verantwortung nur zugeschrieben werden, insoweit eine Person

(durch Handeln oder Unterlassen) Einfluss auf das hat, wofür sie sich zu verantworten hätte. Verantwortung reicht zunächst einmal nur so weit wie der Aktionsradius der Verantwortlichen.

Doch das einfache Entsprechungsverhältnis zwischen Aktionsraum und Verantwortung wird durch die Potenziale von Technik gesprengt. Ein Atomphysiker oder ein Molekularbiologe fühlt sich vielleicht nur für die sorgfältige Durchführung seiner Experimente verantwortlich. Doch was ist, wenn er dadurch die Technologie zur Konstruktion von Atombomben oder menschheitsgefährdende Viren bereitstellt? Der Philosoph Hans Jonas hat in seinem Buch „Das Prinzip Verantwortung“ auf diese Problemstellung reagiert, indem er den kategorischen Imperativ Kants neu formulierte.

E

Exkurs 1.9: Das Prinzip Verantwortung nach Hans Jonas

„Handle so, dass die Wirkungen deiner Handlung verträglich sind mit der Permanenz echten menschlichen Lebens auf Erden“. (22, S. 37)

Technik erhöht die Wirkungsmacht und Reichweite des Handelns – in manchen Fällen bis zur Gefährdung ganzer Lebensformen. Deshalb stellt sie uns vor die Aufgabe, in unserem Handeln nicht nur unmittelbare Folgen zu bedenken, sondern auch Fern-, Neben- und Langzeitwirkungen.

In Bezug auf die Frage der Verantwortung hatte sich die Technikethik ursprünglich hauptsächlich als eine Ethik für das Handeln des Ingenieurs verstanden. Man konzentrierte sich auf die Frage, was es bedeutet, als Hersteller von Technik ethisch zu handeln. Doch Verantwortung für Technik besteht nicht nur bei den Herstellern, sondern ebenso bei den politischen und wirtschaftlichen Akteuren, die die Entwicklung von Technik fördern, sie regulieren und verbreiten. Und sie liegt auch auf Seiten der Nutzer, die Technik erwerben und einsetzen. Technikethik ist also mehr als eine Ethik des Ingenieurshandelns.

D

Definition 1.9: Technikethik

Technikethik ist die Verhandlung der Frage, welcher Einsatz, Förderung, Zulassung und Verbreitung von wie beschaffenen technischen Artefakten und Prozessen gut und gerecht sind und welche nicht.

1.8 Informationsethik

Informationsethik hat es zunächst einmal mit einer sehr allgemeinen Problemstellung zu tun. Denken wir zum Beispiel daran, wie schon der Erfolg von Jägern und Sammlern davon abhängt, zur richtigen Zeit am richtigen Ort zu sein. Kenntnisse darüber, wo gerade Nahrung zu finden ist, können von größter Bedeutung sein. Solche Kenntnisse werden an andere weiter gegeben, vorenthalten, verfälscht oder sie können gegen anderes eingehandelt werden. Information können wir als ein Gut ansehen, für das sich die Frage stellt, wie die Teilhabe an diesem Gut in einer Gemeinschaft geregelt ist. Für eine Gemeinschaft stellt sich die Frage, wer, wann und unter welchen Umständen über welche Informationen verfügen soll. Information kann Insider und Outsider schaffen, sie kann ein Instrument von Macht und Kontrolle ebenso wie von Beteiligung und Kooperation sein. Information kann schädlich wirken, überflüssig, verwirrend und zerstörend ebenso wie befreiend und orientierend. Alle Gesellschaften regeln deshalb Zugänge, Verteilungswege und Schranken in den Informationsflüssen. Und es ist offensichtlich, dass die Frage, wie solche Zugänge, Verteilungswege und Schranken eingerichtet werden sollen, nicht nur eine praktische Frage ist, sondern in hohem Maße eine Frage dessen, welche Form der Regelung jeweils gut und gerecht ist. Die Regelung von Information wirft eine Vielzahl moralischer Fragen auf. Zur Behandlung dieser Fragen bedarf es einer Disziplin der Aushandlung und Debatte. Diese Disziplin bildet ein Teilgebiet der angewandten Ethik, nämlich die Informationsethik.

Informationsethik ist eine relativ junge Disziplin. Warum die Regelung von Informationsflüssen lange Zeit nicht als eigenständiges ethisches Problemfeld angesehen wurde, läßt sich leicht verstehen, wenn wir uns klar machen, dass bis zur Einführung moderner Kommunikationsmittel der Umgang mit Information stets eine Angelegenheit der persönlichen Interaktion war. Die Frage, wie mit Information umzugehen sei, war also gar nicht losgelöst von der Frage, wie man sich gut und gerecht im zwischenmenschlichen Verkehr überhaupt verhält.

Das begann sich zu ändern, als die Druckerpresse es ermöglichte, Schriftstücke in großer Zahl in Umlauf zu bringen, Bücher, und auch Flugblätter und Traktate. Die neuen technischen Möglichkeiten wurden im 16. Jahrhundert von reformerischen und revolutionären Kräften genutzt, während weltliche und kirchliche Machthaber auf Mittel zur Regulierung sannen. Der sogenannte Index, das 'Verzeichnis der verbotenen Bücher' der katholischen Inquisition, wurde 1559, in unmittelbarer Folge der Einführung

moderner Druckerpressen, erstmals erstellt. Auf der anderen Seite forderten Vertreter der Aufklärung freien Zugang zu Büchern für alle Menschen.

Radio und Fernsehen und schließlich das Internet multiplizierten die technischen Möglichkeiten der Beschaffung und Verbreitung von Information. Technik stellt auch hier ein Potenzial dar, das neue Dimensionen ethischer Fragestellung eröffnet. Je mehr durch technische Mittel Information potentiell immer und überall zur Verfügung steht, desto dringlicher stellt sich die Frage, wie die wirkliche Teilhabe an diesem Potenzial auf gute und gerechte Weise zu gewährleisten ist.

D

Definition 1.10: Aufgaben der Informationsethik

Einer der Hauptvertreter der Informationsethik, Rafael Capurro, definiert die Aufgaben der Informationsethik folgendermaßen: „Informationsethik:

- als deskriptive Theorie beschreibt die verschiedenen Strukturen und Machtverhältnisse, die das Informationsverhalten in verschiedenen Kulturen und Epochen bestimmen,
- als emanzipatorische Theorie befaßt sie sich mit der Kritik der Entwicklung moralischen Verhaltens im Informationsbereich. Sie umfaßt: individuelle, kollektive und menschheitliche Aspekte. Sie schließt normative Aspekte ein.“ (8)

Als eine Disziplin, die die Regelung des Umgangs mit Information kritisch reflektiert, ist die Informationsethik mit folgenden Themen befasst:

- Alle Formen der Beschränkung und tendenziösen Steuerung von Informationsflüssen: Die offensichtlichste Form einer solchen Einschränkung ist Zensur. Von Zensur zu unterscheiden sind Verfahren der Selektion. Selektion bedeutet die Auswahl von Information, ihre Zusammenstellung und Zugänglichmachung im Dienste bestimmter Gruppen, Institutionen oder Interessen. Dies geschieht stets auf Kosten anderer Information. Im Internet geht es hier auch um technische Verfahren des Filterns und Blockens, die auf Rating basieren. "Rating ist die Einschätzung und Bewertung von Informationsobjekten bezüglich der Qualität ihrer Inhalte"(26, S. 197). Fragen, nach welchen Kriterien Information bereitzustellen oder vorzuenthalten ist, verbinden die Informationsethik mit den älteren Bibliotheks- und Informationswissenschaften, die eine ihrer Wurzeln darstellen.

- Fragen des geistigen Eigentums, Urheberrechts und der Beschränkung der Kopie und Weitergabe von Information: "Wem gehört Wissen? Wem gehört Information? Darf Wissen überhaupt jemandem gehören, wenn dadurch andere von der Nutzung der aus Wissen abgeleiteten Informationsprodukte ausgeschlossen werden?"(26, S. 10)
- Fragen des Ausschlusses von Information auf Grund sozialer Benachteiligung: Diese Fragen werden mit Hilfe der Unterscheidung von Informationsreichtum (ïnformation rich") und Informationsreichtum (ïnformation poor") diskutiert. Faktoren für eingeschränkten Zugang zu Information können die Gesellschaftsschicht, aber auch Alter und die geographische, politische und ökonomische Situation des Wohnortes eines Informationsteilnehmers sein. Der Preis der erforderlichen technischen Geräte und die Anforderung an eine öffentliche Infrastruktur schließt beispielsweise viele Menschen in Entwicklungsländern von der Teilhabe am "World Wide Webäus.
- Fragen der Regulierung des Verhaltens im Internet, Selbstkontrolle, Moderation, Ethikkodizes und Verhaltensrichtlinien ("Netiquette"). Die Internet Community entwickelt verschiedene Verfahren der Reflexion und Beeinflussung von dienlichem und schädlichem Verhalten im Internet. Die Informationsethik begleitet diese sich autonom weiter entwickelnden Regulierungen in Form kritischer Beobachtung und Kommentierung.

Näheres zu diesen Punkten erfahren Sie im Studienbrief (2.) „Informationsethik und Sicherheitsrationalität“.

K

Kontrollaufgabe 1.5: Informationsethik

Geben Sie Beispiele, an welchen Punkten der vier genannten Themen der Informationsethik herkömmliche Werte berührt werden und an welchen Punkten sich ethische Probleme speziell aus den neuartigen Potentialen der Informationstechnik ergeben.

1.9 Zusammenfassung

Dieser Studienbrief gab Ihnen einen Überblick über das Thema Ethik und ging am Ende auf die Informationsethik ein. So wurden zunächst grundlegende Begriffe definiert und die Zusammenhänge zu Moral und Recht verdeutlicht. Im Kapitel 1.4 Moral, Ethik und Recht im Beruf wurden die

moralischen Regeln in bestimmten Gruppen näher betrachtet und in Gesellschaftlichen Zusammenhang gebracht. Im darauffolgenden Kapitel 1.5 Ethische Theorien wurden verschiedene Ethikformen erläutert. Dazu lernten Sie den Utilitarismus, die Deontologie und die kompetenz- und situationsbezogene Ethiken näher kennen.

Das Kapitel 1.6 Ethischer Relativismus verdeutlichte die unterschiedlichen moralischen Wertvorstellungen und zeigt, dass diese Vorstellungen ständig mit denen von anderen Personen in Konflikt geraten. Sie bilden gleichzeitig die Grundlage für die Interpretationen und Handlungen von jeder einzelnen Person.

Im vorletzten Kapitel 1.7 Technikethik wird entgegen dem Umgang der Menschen miteinander die Bedeutung von Technik in der Gesellschaft erläutert. Insbesondere die Einführung von neuen Technologien bzw. die Weiterentwicklung birgt ein Konfliktpotenzial, das in diesem Kapitel näher betrachtet wird.

Im letzten Kapitel 1.8 Informationsethik lernten wir die Bedeutung von Informationen und welche Macht und Kontrolle von ihr ausgeht kennen. Somit bildet die Informationsethik eine Disziplin für die Schaffung eines gerechten Zugang zu Informationen einer Gesellschaft. Dabei deuten die Fragen am Ende des Kapitel bzgl. Zensur, geistigen Eigentum, Ausschluss von Information auf Grund sozialer Benachteiligung und „Netiquette“ auf die Probleme der Informationsethik an.

1.10 Übungen

Ü

Übung 1.1: Bzgl. des Textes von Dieter Grimm

1. In welchem Sinne lässt sich die Position des ethischen Relativismus mit dem Grundgesetz vereinbaren, gemäß der Darstellung von Dieter Grimm?
2. Nennen Sie Punkte, an denen das Grundgesetz die Orientierung an kulturellen Richtlinien beschränkt.
3. Wie unabhängig ist das Grundgesetz selbst von kulturellen Werten?
4. Welche Typen von Ethik können Sie in Grimms Argumentation ausmachen?

Ü

Übung 1.2: Bzgl. der Abb. 1.1

1. Erläutern Sie in Bezug auf vier Relationen die jeweiligen Ziel-Mittel bzw. Konkurrenzbeziehungen.
2. Geben Sie Beispiele, unter welchen Umständen die erläuterten Ziel-Mittel-Beziehungen auch Konkurrenz beinhalten und wie Unvereinbarkeiten in Konkurrenzbeziehungen aufgelöst werden.

Studienbrief 2 Informationsethik und Sicherheitsrationalität

2.1 Lernziele

Was wird Ihnen vermittelt?

Dieser Studienbrief soll einen genaueren Eindruck des Konflikts zwischen Sicherheit und Freiheit vermitteln. Dabei sollen die Grundlagen dieses Konflikts ebenso sichtbar gemacht werden wie deren Gestalt in informationstechnischen Kontexten und der Bezug zur Informationsethik. So können die in diesem Spannungsfeld immer wieder auftretenden Konflikte besser verstanden und antizipiert sowie idealerweise durch kluges und freiheits- beziehungsweise sicherheitssensibles Agieren vermieden werden.

2.2 Advanced Organizer

Dieser Studienbrief schildert den Konflikt von Freiheit und Sicherheit in der Informationstechnik und unter Bezug auf die Informationsethik. Er bezieht sich auf Grundlagen des vorangegangenen Studienbriefes zu Grundlagen der Informationsethik und bildet eine weitere Grundlage für folgende Studienbriefe.

2.3 Sicherheit als Wert

Definitionsproblematik Sicherheit

Was ist Sicherheit? Diese Frage muss zuerst gestellt werden. Sie zu beantworten wirft uns zunächst auf Definitionsfragen. Tatsächlich ist der Begriff der Sicherheit nur schwer genau zu definieren. Sicherheit ist eines der ältesten Probleme der Menschheit. Daher ist der Begriff naturgewachsen, so dass verschiedene Autoren, verschiedene Kulturen oder gesellschaftliche Gruppierungen ganz eigene Konzepte damit verbinden. Wir können allerdings einige Grundlinien zu einer Definition anführen.

Einmal kann Sicherheit negativ definiert werden. Dies ist die mit unseren Intuitionen am ehesten übereinstimmende Festlegung. Sicherheit ist die Abwesenheit von Gefahr. Diese Definition ist negativ, weil sie den Begriff mit der Abwesenheit eines Zustands beschreibt. Während bei dieser vorerst einfachen Beschreibung allerdings noch jeder zustimmen wird, scheiden sich die Geister bereits, wenn es darum geht zu bestimmen, was Gefahr ist. In einem sehr strikten Sinne kann man hier zunächst die physische Gewalt anführen. Physische Gewalt wird von vielen Menschen als Gefahr verstanden. Gewalt ist etwas, das uns in unserem Empfinden von Sicherheit erschüttert. Davon abgesehen könnten aber noch verschiedene andere Dinge als Gefahren klassifiziert werden. Ein Beispiel sind Umweltgefahren. Ein Sturm, der einen Baum auf ein Haus stürzen lässt, wird auch als Bedrohung der Sicherheit wahrgenommen. Allerdings gilt hier ein anderer Begriff von Sicherheit. Hier kommt eine Nuance ins Spiel, die sich im Amerikanischen in einer Unterscheidung des Begriffs Sicherheit in „Safety“ und „Security“ abbilden. Sicherheit gegen Naturkatastrophen oder auch Unfälle wird dabei unter dem Begriff der „Safety“ behandelt. Sicherheit gegen bewusste, intentionale Angriffe anderer Personen dagegen wird als „Security“ beschrieben. Dieser letzte Umstand ist es natürlich, auf den wir zielen, wenn wir uns mit Sicherheitspolitik, mit Strafverfolgung und mit militärischer Verteidigung befassen. Es geht um Menschen als Gefahr, um Angreifer mit Intentionen. Sicherheit ist also die Abwesenheit von Gefahr durch intentionale Angreifer. Die nächste Frage ist nun, wie weit wir den Gefahrenbegriff eventuell

noch ausweiten müssen. Hier ist insbesondere eine akademische Differenzierung der Begriffswahl zu nennen, die von Galtung eingebracht wurde. Galtung genügt es nicht, von Gewalt nur dann zu sprechen, wenn tatsächlich physische Gewaltakte stattfinden. Er verweist insbesondere im Kontext internationaler Sicherheitspolitik darauf, dass auch andere Aktivitäten von Menschen gegen Menschen gewaltähnliche Wirkungen nach sich ziehen können wie Krankheit, Armut und Tod. Beispiele hierfür sind etwa Wirtschaftssanktionen gegen ein Land, die dieses Land in die Armut zwingen und Hungersnöte mit Toten nach sich ziehen. In diesem Fall wurde mit der Wirtschaftssanktion keine unmittelbare physische Gewalt angewandt. Aber die Wirkungen der Sanktionen sind in letzter Konsequenz ähnlich, so dass auch hier eine Anwendung des Begriffs der Gewalt stattfinden kann. Bei genauer Betrachtung allerdings stellt sich heraus, dass dieser galtungsche Begriff sich eher auf die Gewaltmittel bezieht. Wenn also keine Faust oder keine Waffe, sondern eine Sanktion eingesetzt wird, die Folgen aber Tod, Krankheit und Verletzung sind, soll ebenfalls von „Gewalt“ gesprochen werden können. Dies ist eine schwierige Variation, denn sie weicht den Begriff der „Gewalt“ weit auf. Die Debatte um Galtungs Begriffsführung soll allerdings hier nicht geführt werden. Der Einfachheit und Klarheit halber werden wir im Folgenden von einem Gewaltbegriff ausgehen, der sich auf direkte, intentionale, existentielle Gefahren bezieht.

Galtungs Begriffsdefinition von Gewalt

Zwei Ergänzungen sollen hinzukommen. Einmal soll es als (definitorisch) legitim erachtet werden, auch Gefährdungen der Werte und Wertordnungen hier einzubeziehen. Nicht selten ist nämlich dies gerade ein Grund für gewalttätige Konflikte, da diese Gefährdungen eben oft als existentiell empfunden werden. Dann werden wir Sicherheit nicht nur als Sicherheit vor physischer Gewalt verstehen, sondern auch als Sicherheit unseres Hab und Guts. Dies ist eine legitime Ergänzung. Zum einen können Gefährdungen unseres Besitzes ebenfalls potentiell existentielle Züge annehmen. Zum anderen entspricht sie unseren Intuitionen über Sicherheit. Diese sind etwa klar durch die Gesetzgebung abgebildet, die Aktivitäten in Richtung Diebstahl, Erpressung, Betrug und ähnliches ebenfalls als Verletzung der Sicherheit ausweisen. Hier hätten wir also eine Variante von Gewalt, die tatsächlich nicht mehr im engeren Sinne physische Gewalt widerspiegelt, sondern Gewalt gegen andere Dinge ist, die sich erst mittelbar negativ gegen uns auswirkt. Allerdings ist in unserem Rechtskontext der Zusammenhang mit der Gewalt nicht die unmittelbar bindende Komponente in dieser Interpretation. De facto geht es hierbei um Gerechtigkeit. Gerechtigkeit ist dabei so verstanden, dass sie in einem gesellschaftlichen Vertragswerk, dem

Sicherheit des Hab und Guts

politischen und gesetzlichen Kanon, verankert ist, und dass ein Verstoß gegen diesen Gerechtigkeitskanon als Bruch der öffentlichen Sicherheit geahndet werden kann. Sicherheit drückt also auch die Zuverlässigkeit des Gesellschaftsvertrags aus. Auch hier kann mittelbar eine existentielle Gefährdung identifiziert werden – was exakt der Grund für die vertragliche Vereinbarung ist. Gesellschaften haben sich oft gegründet, um Sicherheit gegen andere zu erlangen. Ohne Gesellschaftsvertrag befinden wir uns im sogenannten „Naturzustand“. Hier hat nur noch der Stärkere Recht, und zwar das, das er sich – im Zweifelsfalle mit Gewalt – nimmt. Dabei genügt nach Thomas Hobbes – dem großen Sicherheitsphilosophen – bereits die Möglichkeit solcher Gewalt, um einen allgemein durch Gewalt determinierten Gesellschaftszustand hervorzubringen.

Gründung von Gesellschaften zur Sicherheit gegen andere

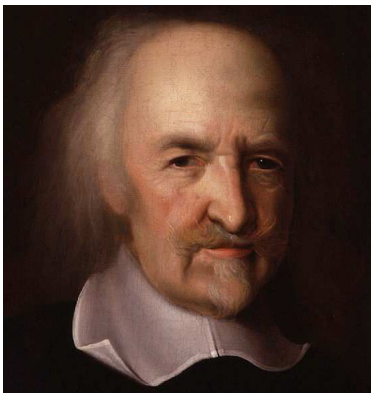


Abb. 2.1: Thomas Hobbes, 1588 - 1679

Quelle: http://de.wikipedia.org/wiki/Hobbes

E

Exkurs 2.1: Hobbes zur Ehrenrettung

Hobbes' Aussagen wurden übrigens gründlich und konsequent missverstanden. Fast alle Werke der politischen Philosophie oder der Sicherheitsforschung benennen ihn als einen Misanthropen. Vor seinen Erfahrungen mit dem englischen Bürgerkrieg habe er den Menschen unterstellt, sie seien durchweg bösartig und auf eigene Vorteile und Konflikte aus. Dass die beiden folgenden Zitate seine bekanntesten sind, illustriert diese Einschätzung. Für den Menschen gilt: „[…] homo homini lupus“(18, Epistola - Dedicatoria S. VI) (der Mensch ist des Menschen Wolf) und: der Naturzustand des Menschen sei ein „[…] bellum omnium contra omnes […]“(18, Praefatio ad lectores S. 16) (Krieg aller gegen alle). Es ist unmittelbar klar, dass dieses Bild vom Menschen zu dunkel gezeichnet ist. Menschen sind auch hilfreich, sozial, altruistisch. Diese Verhaltensweisen sind (in Friedenszeiten)

sogar weit häufiger anzutreffen als egoistisches, unsoziales, schädigendes Verhalten.

War Hobbes also im Unrecht? War er nicht. Er ist nur vielfach falsch gelesen worden. Seine beiden Aussagen bezogen sich auf den Menschen im „Naturzustand“. Der Naturzustand ist allerdings keine Beschreibung des „natürlichen Menschen“. Diese Fehlinterpretation ist vermutlich der Hintergrund vieler falscher Hobbes-Rezeptionen. Er beschreibt lediglich einen hypothetischen Zustand, in dem Menschen ohne jede Form der Herrschaft miteinander leben müssen. Dass dies kein „natürlicher“ Zustand ist, kann leicht erkannt werden. Menschen lebten und leben immer in Herrschaftsverhältnissen. Seine Aussagen über den Menschen waren also auch keine Aussagen über den natürlichen Menschen. Es waren hypothetisch-konditionale Aussagen darüber, wie eine Menschheit beschaffen sein müsste, wenn es keine Herrschaft gäbe. Sie bezeichnen also keinen Glauben von Hobbes darüber, was der Mensch wirklich ist. Sie umschreiben logisch entwickelte Konsequenzen der Abwesenheit einer übergeordneten Instanz der Herrschaft.

Das Argument ist einfach. Wenn es keinen Herrscher gibt, keine Gerichte und keine Polizei, können sich Menschen prinzipiell immer gegenseitig angreifen und überfallen. Sie haben ja keine sichere Bestrafung zu befürchten, sondern nur das, was ihnen ihr jeweiliger Gegner entgegen zu setzen hat. Dass Menschen dies auch tatsächlich tun, liegt einmal in der Natur der Konflikte (mit der Hobbes sich detailliert beschäftigt) und ist außerdem empirisch belegt und bekannt. Dies sind also drei unzweifelhafte Prämissen: Ohne Herrschaft gibt es keinen Schutz vor Gewalt, für Gewalt gibt es viele Gründe und Gewalt existiert. Man könnte noch hinzufügen: Menschen haben Abscheu vor einem gewaltsamen Tod.

Diese Prämissen gelten unabhängig von Menschenbildern, also von Annahmen darüber, wie das menschliche Wesen beschaffen ist. Auch wenn jeder grundsätzlich gut, zuvorkommend und altruistisch wäre und Gewalt nur ein äußerst extremes Phänomen, könnte prinzipiell ein Missetäter vorbeikommen und alle töten.

Außerdem sind auch alle Verabredungen, Verträge und langfristig

oder kostenintensiv aufgebauten Güter in dieser Situation nur noch von begrenztem Wert. Verträge können jederzeit gebrochen werden, wenn keine Vorteile aus ihrer Einhaltung resultieren. Wer sollte den Vertragsbrecher bestrafen? Und zeit- und kostenintensive Güter könnten jederzeit entwendet werden. In sie zu investieren wäre ein hohes Risiko.

Was ist also die Folge? Wenn es prinzipiell sein könnte, dass einem jederzeit Gewalt und Willkür widerfahren und wenn man dies unbedingt vermeiden möchte, ist es also nötig, sich darauf einzustellen. Diese Einstellung muss sich als Wille zur Verteidigung, also als physische und psychische Bereitschaft zum Kampf formieren. Andere Möglichkeiten gibt es in der hypothetischen Abwesenheit von Herrschaft nicht. Da das Risiko außerdem auch bei einer grundlegend guten Menschheit, also einer geringen Eintrittswahrscheinlichkeit von Gewalt, hoch ist (der Schaden ist immerhin der eigene Tod), ist Vorsicht besser als Nachsicht. Viele Menschen werden also eine eher hohe Bereitschaft zur Selbstverteidigung an den Tag legen, vor allem Fremden gegenüber. Eventuell – in Zweifelsfällen, die vorangegangenen Erfahrungen mit Konflikten strukturell gleichen – werden sie auch präventiv zuschlagen. Dass der Mensch im Naturzustand also – prinzipiell – des Menschen Wolf ist, ist eine rein logische Konsequenz der Anfangsbedingungen. In der Abwesenheit von Herrschaft muss sich jeder sicherheitshalber in einer andauernden Kampfbereitschaft befinden. Der Menschenwolf muss nicht beißen. Aber er muss bereit sein, zu beißen.

Das ist das Argument von Thomas Hobbes. Sicher hat er Gewalt als alltäglicher erlebt als heutige Westeuropäer. Aber für seinen Schluss ist kein negatives Menschenbild nötig. Es wird auch keines impliziert. Seine Folgerungen sind logische Optionen des Handelns aus allgemeinen Prämissen. Es ist keine Referenz auf eine gute oder schlechte Menschheit nötig.

Auch eine misanthropische Interpretation des zweiten Zitats lässt sich schnell entkräften. Der vorangegangene Teil hatte bereits festgestellt, dass Menschen ohne Herrschaft keine externe Absicherung gegen Gewalt haben und deshalb selbst im Zustand andauernder Kampfesbereitschaft stehen müssen. Nun soll die Stelle des Zitats in

ihrer Gänze zitiert werden: „[…] during the time men live without a common Power to keep them all in awe, they are in that condition which is called Warre; and such a warre, as is of every man, against every man. For Warre, consisteth not in Battell onely, or the act of fighting; but in a tract of time, wherein the Will to contend by Battell is sufficiently known: and therefore the notion of *time*, is to be considered in the nature of Warre; as it is in the nature of Weather. For as the nature of Foul weather, lyeth not in a showre or two of rain; but in an inclination thereto of many days together: so the nature of War, consisteth not in actual fighting; but in the known disposition thereto, during all the time there is no assurance to the contrary.“ (17, S. 88f).

Die Bemerkungen sind treffend. Von Krieg spricht man als einer ausgedehnten Zeitperiode. Auch wenn nur episodisch gekämpft wird, herrscht Krieg solange gesellschaftlich breit ein Wille zum Kampf da ist und Kämpfe stattfinden könnten. Für eine Menschheit ohne Herrschaft ist aber genau das der allgemeine Zustand. Sie sind dauernd kampfbereit; Gewalt könnte jederzeit ausbrechen. Das gilt überdies nicht nur zwischen zwei erklärten Parteien, sondern zwischen allen Menschen. Dadurch herrscht also die besondere, von Hobbes identifizierte Variante des Krieges: der Krieg aller gegen alle. Der Krieg aller gegen alle ist also ebenfalls keine misanthropische Beschreibung des Ist-Zustandes der Menschheit. Die reale Beschaffenheit der Menschheit ist nicht adressiert und spielt erneut auch keine Rolle.

Deutungen von Hobbes als Misanthrop müssen also als unbegründet zurückgewiesen werden. Er hat kein Menschenbild vorgeschlagen, um seine politische Philosophie zu begründen. Ganz im Gegenteil: Er hat gerade bewiesen, dass Menschenbilder bei der kategorialen Entscheidung zur Einrichtung von Sicherheit und Herrschaft keine Rolle spielen.

Muss man die Möglichkeit der Gewalt jederzeit einbeziehen, befindet man sich in einem dauerhaften Zustand von Angst und Verteidigung, der zumin-

dest auf der Seite der Opfer den Zustand der Gewalt bereits hinreichend realisiert.

K

Kontrollaufgabe 2.1: Gesellschaften

Worin liegt der Mehrwert einer Gesellschaft gegenüber dem Naturzustand?

Neben unserer Variante gibt es noch weitere Definitionsversuche.

D

Definition 2.1: Beispiele für Definitionen von „Sicherheit“

- „Security itself is a relative freedom from war, coupled with a relatively high expectation that defeat will not be a consequence of any war that should occur“(4, S. 102)
- „A nation is secure tot he extent to which it is not in danger of having to sacrifice core values if it wishes to avoid war, and is able, if challenged, to maintain them by victory in such a war“(27, S. 36)
- „National security may be defined as the ability to withstand aggression from abroad“(28, S. 151)
- „A threat to national security is an action or sequence of events that (1) threatens drastically and over a relatively brief span of time to degrade the quality of life for inhabitants of a state, or (2) threatens significantly to narrow the range of policy choices available tot he government of a state or to private, nongovernmental entities (persons, groups, corporations) within the state“(38, S. 133)
- „Security, in any objective sense, measures the absence of threats to acquired values, in a subjective sense, the absence of fear that such values will be attacked“(41, S. 150)
- „Security-insecurity is defined in relation to vulnerabilities – both internal and external – that threaten or have the potential to bring down or weaken state structures, both territorial and institutional, and governing regimes“(2, S. 9)
- „Emancipation ist he freeing of people (as individuals and

groups) from the physical and human constraints which stop them carrying out waht they would freely choose to do ... Security and emancipation are two sides of the same coin. Emancipation, not power or order, produces true security. Emancipation, theoretically, is security“(6, S. 319)

- „If people, be they government ministers or private individuals, perceive an issue to threaten their lives in some way and respond politically to this, then that issue should be deemed to be a security issue“(20, S. 9)
- „Security ... implies both coercive means to check an aggressor and all manner of persuasion, bolstered by the prospect of mutually shared benefits, to transform hostility into cooperation“(25, S. 25)

Nach: Alan Collins, Security Studies, Oxford 2007

Kontrollaufgabe 2.2: Begriffsdefinition Sicherheit

K

Wie lässt sich Sicherheit beschreiben? Warum gibt es so viele unterschiedliche Begriffe von Sicherheit?

Damit wollen wir die definitorische Festlegung wieder verlassen. Es wird klar, dass der Begriff leicht viele verschiedene Konnotationen annehmen kann. Wichtig soll hier vor allem sein, dass eine intentionale Bedrohung, also ein Angreifer und kein natürlicher Umstand, und dass eine potentiell existentielle Bedrohung vorliegt. In diesen Fällen wird Sicherheit ganz allgemein als Abwesenheit dieser Art von Bedrohung verstanden.

Wert der Sicherheit

Der Wert der Sicherheit ist ausgehend von dieser Bestimmung unmittelbar klar. Bedrohungen unserer Existenz sind in unserem Bedrohungsempfinden generell hoch eingewertet. Das ist in gewisser Weise logisch. Zu Existieren ist eine condicio sine qua non für alle weiteren Zustände und deren Gefährdungen, so dass also mit der Bedrohung der Existenz logisch betrachtet eine Universalbedrohung besteht. Logik hat jedoch in diesem Bereich nicht wirklich die ausschlaggebende Rolle. Denn immerhin gibt es ja keinen logisch fassbaren Grund, warum wir überhaupt existieren müssen. Hier kann man nur metaphysische Annahmen walten lassen, und die sind jederzeit durch ihr Gegenteil austauschbar. Logik allein erklärt unsere hohe Bewertung der

Sicherheit also nicht. Gefühle sind da schon wesentlich ausschlaggebender.

Emotion: Angst vor dem Tod

Zuerst ist hier die Angst vor dem Tod zu nennen. Sie ist einfach ein Naturreflex, eine vordeterminierte und biologisch weise Reaktion, die folgend existenzerhaltende Maßnahmen in bessere Weise ermöglicht. Dies gilt bei Tieren wie bei Menschen, bei Menschen allerdings in besonders starker Weise. Menschen haben ein deutlich ausgeprägteres Vorstellungsvermögen. Sie können die Angst vor dem Tod also nicht nur spüren, wenn sie dem Tod unmittelbar ins Auge sehen, sondern auch dann, wenn sie dem Tod imaginativ ins Auge sehen. Sie haben eine Vorstellung vom Tod, von vielen Toden, um genau zu sein, und diese können sie fast genauso ängstigen wie jede unmittelbare Bedrohung. Der Tod ist ihnen damit wesentlich plastischer und näher als Tieren, bedrohlicher und zudem tatsächlich auch in seiner Logik erfahrbar. Viele Menschen denken im Angesicht des Sterbens daran, was sie im Leben noch machen wollten, also an die Klasse der mit dem Tod ausgeschlossenen Handlungen. Diese logische Überlegung muss allerdings dem emotionalen Erleben der Angst gegenüber als nachgeordnet geführt werden. Die Angst vor dem Tod ist eine überaus mächtige Emotion, die einen nicht unwesentlichen Teil der menschlichen Kultur und Zivilisation determiniert.

Trotz dieser logischen und emotionalen Stärke ist der Tod aber nicht notwendig immer die größte Bedrohung. Es gibt im menschlichen Empfinden höhere und wichtigere Dinge als Sicherheit. Das zeigt die immer wieder hohe Bereitschaft, sich für gerechte (oder vermeintlich gerechte) Angelegenheiten in die vergleichsweise hohe Gefährdung des Krieges zu begeben.

Freiheit und Gerechtigkeit

Freiheit und Gerechtigkeit sind die beiden wichtigsten Beispiele für manchmal als höher empfundene Werte. Massive Einschränkungen von Freiheit, bei denen zudem noch mit zweierlei Maß zwischen verschiedenen gesellschaftlichen Klassen gewertet wird, werden oft als so drastisch störend empfunden, dass gegen die Vertreter der Unfreiheit gewaltsamer Protest ausgeübt wird – oft in dieser Form, weil es eben die letzte mögliche Form des Protests überhaupt ist und oft unter Gefährdung der eigenen Freiheit und des eigenen Lebens. Allerdings sind diese Verhältnisse volatil. Verschiedene Kulturen nehmen Hierarchien von Werten anders wahr, andere Zeiten mit anderen Rahmenbedingungen werden vielleicht auch andere

Hierarchien akzeptabel finden. Viel hängt vom unmittelbaren Kontext und vom Empfinden der Akteure ab.

Kontrollaufgabe 2.3: Sicherheitswert

Worin liegt der Wert der Sicherheit?

K

2.4 Prinzipien der Sicherheitsrationalität

Wertvorstellung

Gesellschaftliche Werte kondensieren in vielen Formen. Gesetze sind eine sehr explizite und deutliche Form. In diesem Fall sind die Werte selbst auf einer hohen Gesetzesebene und ihre Anwendungen auf niederen Gesetzesebenen festgelegt. So kann in Fällen von Handlungen, bei denen auf Werte als Orientierung zurückgegriffen werden muss (Gesetze sind gerade dadurch ausgeprägt, dass sie von ihrer entsprechenden Gesellschaft als notwendige Werte verstanden werden) ein Referenzpunkt identifiziert werden, der mal mehr, mal weniger klare Vorgaben macht.

Wertrationalität

Ein anderes, weicheres und schwieriger zu fassendes Kondensat gesellschaftlicher Werte sind Rationalitäten in wertebezogenen Kontexten – Wertrationalitäten. Sie folgen stärker individuellen oder gruppenbezogenen Wertehierarchien und äußern sich in Vorstellungen von relativen Kausalitäten und Relevanzen auf verschiedenen Ebenen. Die Vorstellungen von Kausalitäten sortiert Fakten in Ursache-Wirkungs-Zusammenhänge, deduziert aus Prinzipien, die eine übergelagerte Ordnungsebene bieten. Dazu werden verschiedene Kausalitäten und Prinzipien als relevanter und emotional teils anders als andere empfunden. Dies sind dann stärker subjektive Setzungen, die dann aber auch die eher auf logischer Ebene hergestellten Kausalitäten beeinflussen, indem sie bestimmte Kausalitäten bevorzugen und andere benachteiligen.

Das Zusammenspiel der subjektivistischen Kausalitäten und Relevanzen zeigt sich dann auf verschiedenen Ebenen. Eine bereits angedeutete Ebene etwa ist die kognitive Ebene der Wahrnehmung, Nacherzählung und Einordnung von Ereignissen. Viele Ereignisse werden recht verschieden interpretiert, in ihrer möglichen Geschichte, in Bezug auf die Motivationen der Akteure oder auf die Konsequenzen. Es gibt immer viel Spielraum in der Deutung von Fakten. Ein Datenschutzvorfall etwa wie der zum Zeitpunkt des Schreibens aktuelle und brisante Fall PRISM wird von Datenschützer als große Katastrophe, vor allem aber als „Spitze eines Eisbergs“ wahrgenommen, während der Fall von einigen (glücklicherweise wenigen)

Protagonisten aus der Sicherheitscommunity eher als vielleicht notwendige, in dieser Form aber illegitime Maßnahme und außerdem nicht als Spitze eines Eisbergs, sondern als voller und einziger Eisberg wahrgenommen wird.

Eine andere, wichtige Ebene ist die der Handlungen. Eine wesentliche Funktion bestehender Wertehierarchien ist nämlich die Vorstrukturierung von Handlungen. Die kausalen Gefüge und die emotionalen Setzungen evozieren in wertspezifischen Situationen sofort spezifische Reaktionen, die ein rasches, wertgemäßes Handeln ermöglichen, ohne dass eine Situation lange bewertet werden muss.

Das Konstrukt der Wertrationalitäten – die beiden vorgestellten Ebenen sollen im weiteren als ausreichend gelten und nicht weiter differenziert werden – soll uns nun helfen, das Denken und Handeln der enger mit Sicherheit als zu realisierendem Wert befassten Berufsgruppen und Subkulturen zu verstehen. Denn wenn man mit dem Erhalt eines Wertes spezifisch befasst ist – oft aus Überzeugung – stellen sich in der Regel spezifische Wertrationalitäten ein. Sie werden mit dem Leben innerhalb der spezifischen, mit Sicherheit befassten Gruppe erlernt, teils über Ausbildung und Reflektion, teils durch Überzeugung, teils durch Praxis (wobei letztere aber auch einen gewissen „Abrieb“ bewirken kann).

K

Kontrollaufgabe 2.4: Wertrationalitäten

Was sind Wertrationalitäten? Warum sind Rationalitäten manchmal subjektivistisch?

Was sind nun also die Wertrationalitäten der Sicherheitscommunity? Es lassen sich vier Prinzipien identifizieren.

2.4.1 Prinzip des Schutzes

Das erste Prinzip ist das Kernprinzip der Sicherheit, das des Schutzes. Dabei ist freilich vorläufig freigelassen, was der Schutzgegenstand ist. Es kann die eigene Bevölkerung sein, es kann sich aber auch um bestimmte gegenständliche Werte, um spezifische Gruppen, um abstrakte Werte oder um anderes handeln. Dies ist eine defensiv klingende Variante. Vielen Lesern mag das jetzt zu freundlich erscheinen, da es ja oft immerhin auch Sicherheitskräfte sind, die für Unsicherheit und die Bedürftigkeit nach Schutz sorgen. Das

soll aber mit dieser Beschreibung nicht ausgeschlossen sein. Es ist lediglich im Begriff der Sicherheit angelegt, dass es sich auch um eine Sicherung von etwas Bestehendem handelt, so dass also der Ansatz tatsächlich zumindest konzeptionell immer der der Defensive ist. Das lässt sich übrigens auch in der Sicherheitspraxis feststellen, in der Verargumentierung von Sicherheitsmaßnahmen. In der inneren Sicherheit wird ohnehin vorrangig defensiv argumentiert. Aber selbst bei militärischen Invasionen mit eindeutig aggressivem Charakter wird inzwischen stets ein Verteidigungsfall in irgendeiner Form angerufen, eine Berechtigung zum Eingriff. Diese starke argumentative Komponente ist etwas eher Neues in der Kriegsführung, hat aber am Wesen des Krieges sonst nicht viel geändert.

Im Rahmen der Wertrationalitäten äußert sich dieses Prinzip auf der kognitiven Ebene in der Wahrnehmung sicherheitsrelevanter Vorfälle in bestimmten Strukturen. Variationen nach bestimmten Auftragsformen sind möglich, aber in der Regel bemüht man sich, Ursachen, potentielle weitere Ursachen, vergangenen und zukünftigen Verlauf, Akteure und deren Wirkmacht, Schutzgegenstände und deren Exposition sowie Schutzoptionen relativ zu diesen anderen Korrelata zu erfassen. Auf der Handlungsebene schließlich geht es dann um eine oft möglichst schnelle Umsetzung der erfassten Umstände, wobei der Erfassung selbst häufig eine nachgeordnete Rolle eingeräumt wird. In kritischen Sicherheitssituationen zumindest ist Handeln wichtiger als Denken. Eine andere Kategorie dagegen sind Vorbereitungen für Handlungen in Sicherheitssituationen, die keine unmittelbare, sofortige Reaktion erfordern. In solchen Situationen bemüht man sich zumeist, den zeitlichen Rahmen möglichst vollständig zu einer kognitiven Erfassung der Situation zu nutzen, um so möglichst effizientes Handeln folgen zu lassen. Dabei kann dann allerdings auch entschieden werden, bereits früher einige Steuerungshandlungen zu initiieren, durch die der Verlauf günstig für Folgehandlungen geändert wird.

2.4.2 Prinzip der Dominanz

Das zweite Prinzip ist ein Realisierungsprinzip gegenüber dem ersten Prinzip des Schutzes. Um Schutz relativ zu einer Bedrohung entfalten zu können, muss man sich in eine dominante Position gegenüber dieser Bedrohung bringen. In den meisten Fällen ist das eine physische Dominanz. Der Beschützer muss der Bedrohung in physischer Gewalt überlegen sein. Dazu gehört allerdings nicht die reine Wirkmächtigkeit möglicher Wirkmittel wie Waffen, sondern auch – ganz im Sinne eines soziotechnischen Ver-

ständnisses – deren Form der Nutzung auf taktischem, strategischem und politischem Niveau. Ein Gegner wie eine Guerillaarmee kann einer staatlichen, regulären Armee an Waffen und konkreten Mitteln hoffnungslos unterlegen sein und dennoch durch geschicktes Taktieren auf verschiedenen Ebenen siegreich, also dominant. Daraus folgt also, dass eine optimale Fusion von Sicherheitsmitteln und deren Anwendung auf verschiedenen wirksamen Ebenen erreicht werden muss, wobei sich das Optimum gerade relativ an der Aufgabe misst. Zu diesem Punkt als „ausführendem" Prinzip der Sicherheit gibt es eine reichhaltige Literatur in der Philosophie und allgemein der Theorie des Krieges, von Sun Tsu zu Clausewitz oder anderen, moderneren Autoren zu Taktik und Strategie, in der inneren wie in der äußeren Sicherheit.

2.4.3 Prinzip der Verantwortung

Ein weiteres Prinzip der Sicherheitsrationalität ist das der Verantwortung. Verantwortung bedeutet in diesem Kontext, in einigen ausgezeichneten Kontexten Handlungszuständiger zu sein. Der Soldat etwa ist ausgewiesener Handelnder des Krieges, der Polizist ausgewiesener Handelnder der inneren Sicherheit. Als ausgewiesene Akteure dieser Kontexte kommt ihnen innerhalb der entsprechenden Umstände eine Handlungsvollmacht, aber auch eine Handlungspflicht zu. Sie dürfen und sie müssen handeln. Anderen Akteuren dagegen ist ein Handeln in den entsprechenden Situationen in der Regel untersagt. Ein Krieg ist natürlich eine in gewisser Weise recht regelfreie Situation. Jedoch darf auch dort – zumindest theoretisch – nicht einfach jeder jeden umbringen, der zu einer gegnerischen Kraft gehört. Er muss ordentlicher Angehöriger einer Streitkraft und idealerweise durch eine Uniform und ähnliche Dinge auch als solcher ausgewiesen sein. Noch strenger als diese Regelungen sind normalerweise die Regelungen der inneren Sicherheit. Hier ist „Selbstjustiz" in den meisten Gesellschaften noch wesentlich stärker ausgeschlossen als im Falle des Krieges. Als destabilisierendes und sicherheitsgefährdendes Element steht sie in der Regel selbst unter Strafe.

Die spezifischen Mengen von Rechten und Pflichten sind oft recht feingranular in Vorschriften und Gesetzen oder Befehlsketten festgehalten. Verantwortung hat also in diesen Kontexten nicht nur eine optative Rolle wie für Zivilisten im täglichen Leben, in dem man sich frei entscheiden darf, ob man in verantwortungsbedürftigen Situationen auch Verantwortung übernimmt oder nicht. Sie ist ein festes und expliziertes Regelelement.

Neben diesen festen und ausgesprochenen Elementen lassen sich aber auch weiche Faktoren ausmachen, die nicht eindeutig festgelegt sind. Das Ausmaß der Wahrnehmung der Verantwortung in einigen Situationen etwa ist absichtlich nicht hochpräzise festgelegt, da so eine Festlegung einerseits schwierig für alle Situationen zu antizipieren wäre und da andererseits der Verantwortungshandelnde durchaus einigen Interpretationsspielraum haben soll, um in entsprechenden Situationen angemessen handeln zu können und eventuell stärker oder weniger stark agieren zu können.

2.4.4 Prinzip der Verantwortlichkeit

Zum Prinzip der Verantwortung gehört das Prinzip der Verantwortlichkeit. Als „Verantwortlichkeit“ wird der genauere Kanon der Rechte und Pflichten der Verantwortung und die Verpflichtung auf diesen Kanon gefasst. Verantwortlichkeit drückt die Verpflichtung eines verantwortungsartig Handlungszuständigen auf seine Aufgabe und deren einrahmende Elemente aus, die sich unter anderem in einer juristischen oder anderweitigen Rechenschaftspflicht des Verantwortlichen für seine Handlungen äußert.

Im Rahmen der Verantwortlichkeit lassen sich ebenfalls weiche Faktoren ausmachen, die nicht eindeutig festgelegt sind. Das Ausmaß der Verantwortlichkeit etwa ist etwas, das durchaus Interpretationsspielraum hat.

Mit diesen Prinzipien soll die Sicherheitsrationalität grundlegend umrissen sein. Natürlich gäbe es zu diesem Thema noch viele weitere, interessante Dinge zu sagen und viele weitere Unterscheidungen zu machen. Für den aktuellen Zweck aber soll es bis hierhin reichen. Wir können als Essenz des Gesagten festhalten, dass Sicherheitshandelnde (zumindest formelle Sicherheitshandelnde) eine Aufgabe des Schutzes wahrnehmen, die sie durch eine Dominanz von Macht realisieren, wobei sie auf bestimmte Kataloge von Rechte und Pflichten verpflichtet und ihrem Handeln gegenüber rechenschaftspflichtig sind. Dabei ist in dieser Festsetzung noch nichts darüber gesagt, was geschützt wird und welche Kataloge von Rechten und Pflichten mit welcher Schärfe in Bezug auf die Rechenschaftspflicht zur Anwendung kommen. Dies sind Variablen, die sich in unterschiedlichen Gesellschaften und teilweise sogar je nach Situation ändern können. Diese Variabilität ist zum einen notwendig, da Gesellschaften mit ihren Sicherheitsorganen auf veränderte Bedingungen auch anders reagieren müssen. Es ist aber auch eine der wesentlichen Schwierigkeiten der Sicherheit, denn hier schlummert

das allseits bekannte Potential der Sicherheit, in ihr Gegenteil, in Unsicherheit umzuschlagen.

K

Kontrollaufgabe 2.5: Prinzipien der Sicherheitsrationalität

Was sind die Prinzipien der Sicherheitsrationalität und wie hängen sie zusammen?

2.5 Sicherheit und Freiheit

Dieses Potential soll uns im nun folgenden Abschnitt insbesondere im Kontext zu Freiheit beschäftigen. Zuerst aber wollen wir ein paar allgemeine Überlegungen dazu anstellen. Wie wird Sicherheit realisiert? Wie genau drückt sich die Dominanz aus? In gewisser Weise ist Dominanz immer die Möglichkeit der höheren physischen Gewalt. Zwar stehen vor dieser letzten Option immer viele Zwischenoptionen. Bei einer regulären inneren Sicherheit in einem funktionierenden und verhältnismäßig friedlichen Land etwa würde man denken, dass die Sicherheit auf einer friedlichen Gesellschaft, ihrem Wohlstand oder auf ihrer Verfassung beruht, nicht auf dem Potential physischer Gewalt. Aber solche Bewertungen täuschen. Was etwa sollte selbst in einer friedlichen Gesellschaft oder in einem wohlständigen Land weniger friedliche oder wohlständige Bevölkerungsteile oder Bevölkerungen davon abhalten, sich auf Kosten anderer zu bereichern? Und was sollte einen Teil des Staates oder andere Gruppierungen davon abhalten, sich von einer Verfassung zu entfernen und einen Landstrich mit eigenen Regeln zu eröffnen? In diesen Fällen muss eine real physische Instanz existieren, die zur Not mit höherer Macht einschreiten und durch die Verursachung von Tod oder Unfreiheit gesellschaftlich ungewollte Handlungen abstellen kann. Sicherheit in Form der physischen Dominanz ist also eine notwendige Komponente für jeden Staat.

Man kann philosophisch darüber räsonieren, ob es einmal einen Gesellschaftszustand geben kann, indem rein auf Basis vernünftiger Einsicht der Frieden unter allen Umständen als höchstes Gut erachtet und wechselseitig eingehalten wird. Dies war zumindest ein wesentliches Argument Immanuel Kants.

Aber das ist zweifelhaft. Die menschliche Natur erachtet viele Dinge als „vernünftig“, darunter auch die Vernichtung anderer Menschen zum Zwecke der Bereicherung. Und das kann sogar moralisch vernünftig sein. Die Selbstverteidigung etwa ist etwas, das in den meisten Moralphilosophien

Abb. 2.2: Immanuel Kant, 1724 - 1804

Quelle: http://en.wikipedia.org/wiki/Immanuel_Kant

als immer legitim erachtet wird. Schließt diese Selbstverteidigung die Eroberung eines Landes oder verschiedener Frachter ein, indem etwa eine Hungersnot in einem Landstrich ausgelöst wurde, so ist ein unter diesen Umständen stattfindender Mord und Todschlag zumindest nicht vollkommen verwerflich. Es kommt dabei natürlich noch auf weitere Rahmenbedingungen an. Utilitaristisch etwa könnte man hinzufügen, dass das Ausmaß des Elends durch eine Invasion nicht größer sein sollte als durch die Hungersnot. Außerdem sollten – deontologisch – Völker- und Menschenrechte beachtet werden. Davon abgesehen aber können Ressourcenkriege eben durchaus vernünftig sein. Die meisten aktuellen Ressourcenkonflikte sind es natürlich nicht. Bei ihnen, wie etwa bei den Kriegen um Öl und andere Energieträger, geht es nämlich eben nicht um das blanke Überleben, sondern um das Leben auf einem gewissen Lebensstandard. Dies ist weit weniger legitim und stößt daher auf immer wieder auf berechtigten Protest. Aber das führt uns nun zu weit weg.

Ressourcenkonflikte

Hier wollen wir lieber weiter die Notwendigkeit der physischen Dominanz als Grundlage der Sicherheit betrachten. Dabei lässt sich jetzt einwenden, dass es bei Sicherheit nicht vorrangig um reale Dominanz, sondern um die *Möglichkeit* der Dominanz, um die Bedrohung geht. Da Menschen kognitive, wissensbegabte und zudem ihr Leben in die Zukunft entwerfende Lebewesen sind, ist dies eine bereits ausreichende Komponente in menschlichen Gesellschaften, um als Regulativ der Sicherheit zu wirken. Die Vorstellung von Tod und Unfreiheit ist für Menschen in der Regel bereits ausreichend, um sie von Taten abzuhalten, die eben diese unangenehmen Zustände hervorrufen könnten.

Physische Dominaz

Ökonomische Basis von Konflikten

Für die Sicherheit ist das ein günstiger Umstand. Da die Angst vor der Strafe genügt, muss nicht jedes Mal real bestraft werden. Es genügt die diffuse Unsicherheit eines Täters oder einer gegnerischer Streitkraft, ob nicht die Kosten höher sein werden als der Nutzen. Die meisten Formen von Konflikten rechnen auf dieser ökonomischen Basis, auch wenn die Werte nicht unbedingt monetär sein müssen. Strategisches Denken ist inhärent ökonomisch. Insbesondere im militärischen Bereich spielt in diese Unsicherheit auch eine starke kognitive Komponente hinein. Dort geht es nicht nur darum, real die Möglichkeiten der Bestrafung zu demonstrieren, sondern auch, potentielle Gegner im Unklaren über das eigene Potential zu lassen. Ältere und noch „kriegsfreundlichere“ Strategen wie Sun Tsu empfehlen dabei eine umgekehrte Proportionalität. Ist man schwach, soll man stark scheinen (damit man nicht angegriffen wird), ist man dagegen stark, soll man schwach scheinen (damit man angegriffen wird und seinen Gegner vernichten kann). Auch bei der inneren Sicherheit spielt die kognitive Unsicherheit eine Rolle, allerdings ist sie dort schwächer ausgeprägt, da die Machtverhältnisse klarer sind. Eine Polizei muss keine Stärke vortäuschen, sie ist in der Regel stärker als die Kriminalität. So sind auch Auslandsnachrichtendienste als „Aufklärer“ dieser Unsicherheiten immer noch bedeutsamer als Inlandsnachrichtendienste.

Das rechte Maß für die Sicherheitswirkung

Um also eine Sicherheitswirkung zu erhalten, muss das Maß der Angst vor höheren Kosten als Nutzen ausreichend sein. Dieses Maß speist sich aus zwei Konstituenten: der Realisierbarkeit der Bestrafung und die Höhe der Strafe sowie in einigen Fällen auch der Umstand, ob und wie die Konsequenzen für den entsprechenden Handelnden persönlich wirksam werden oder nicht. Ist eine Strafe nicht realisierbar, indem etwa keine ausreichenden Polizeikräfte vorhanden sind oder indem eine Armee nicht schlagkräftig ist, so entfalten diese Elemente keine Sicherheitswirkung, da sie keine ausreichende Angst generieren. Sind die Strafen zu niedrig, so dass man sie als potentielle Kosten billigend in Kauf nehmen kann, entfaltet sich ebenfalls keine Sicherheitswirkung, da der Nutzen sicherheitsgefährdenden Handelns mitunter beträchtlich ist. Man muss also ein rechtes Maß finden.

Neben Sicherheit auch Wohlstand

Dieses rechte Maß ist nun allerdings nicht automatisch das Maximum der Bestrafung – eine Riesenarmee und Polizei mit Höchststrafen. Dies entfaltet zwar erhebliche Sicherheit, hat aber diverse Nebenwirkungen, denn natürlich ist Sicherheit nicht alles, was wir im Leben wollen. Wir möchten auch gerne in Wohlstand leben – und große Sicherheitskräfte haben von

jeher erheblich am Wohlstand gezehrt – vor allem möchten wir aber auch in Freiheit leben. Freiheit ist ein Grundbedürfnis des Menschen. Es gibt zwar viele formelle Freiheiten wie die Freiheit der Wahl oder die Freiheit der Presse, die man immer wieder gerne zitiert, wenn man Freiheiten rechtfertigen oder ausweisen muss. Aber grundlegend für jeden gesellschaftlichen Willen nach Freiheit ist das Bedürfnis des Einzelnen nach Freiheit. Wie genau diese Freiheit aussieht, wie umfangreich sie ist und in welchen Typen von Handlungen man sie realisiert sehen möchte – denn Freiheit ist letztlich immer Handlungsfreiheit – ist erneut unterschiedlich je nach Kultur oder gesellschaftlicher Situation. Die Freiheit aber, auf die man sich kulturell und gesellschaftlich verständigen kann, muss folgend auch gesellschaftlich garantiert werden können.

Dabei ist nun die Sicherheit ein ganz besonderes Korrelat. Einmal ermöglicht sie Freiheit. Dies ist etwas, das von Freiheitskämpfern immer wieder gern im Misskredit gebracht wird. Aber eine Gesellschaft ohne Sicherheit, die sich also in einem hobbesschen Naturzustand befindet ohne regelnde und Regeln instanziierende Kräfte, ist auch eine Gesellschaft mit zumindest eingeschränkter Freiheit, denn dort herrscht nur das Recht des Stärkeren als vollkommen willkürliches Naturrecht. Einigen gefällt so etwas – den Stärkeren. Andere dagegen – die Schwächeren – erleben einen Naturzustand ohne eine kantische Vernunfteinsicht zum Frieden als Tyrannei und maximale Unfreiheit. Ein Grundmaß an Sicherheit, das zumindest Willkür der Stärkeren ausschließt, ist also eine notwendige Bedingung für ein gesellschaftlich breites Maß an Freiheit. Andererseits aber kann Sicherheit Freiheit auch wieder eingrenzen. Totalitäre Staaten sind hier das Extrembeispiel. Bei ihnen ist der Wert der Sicherheit, der Stabilität übergreifend wichtig und dominierend und erlaubt diverse Einschränkungen der Freiheit. Diese Einschränkungen sind nicht willkürlich. Sie folgen immer noch der Idee der gesetzlichen Regulierung, den vier Prinzipien der Sicherheitsrationalität, und sind von daher keine Instanzen eines hobbesschen Naturzustands. Aber sie bewirken dennoch erhebliche Einschränkungen in Handlungsfreiheiten.

Systematisch steht man hier vor einem Dilemma. Denn die Möglichkeit der Sicherheit ist nicht anders zu realisieren als Möglichkeit der Einschränkung der Möglichkeit der Freiheit. Es geht in beiden Fällen um Handlungsfreiheiten. Der Wert der Freiheit betont die Möglichkeit des freien Handelns in bestimmten Feldern und unter bestimmten Bedingungen. Der Wert der Sicherheit muss als Möglichkeit der Einschränkung des freien Handelns in bestimmten Feldern und unter bestimmten Bedingungen realisiert werden.

Es hängt also alles an den Festlegungen der Felder, der Typen von Handlungen, sowie der Bedingungen. Davon ausgehend werden Ausmaß und Art der Sicherheit und damit – u.E. ex negativo – Ausmaß und Art der Freiheit festgelegt.

Beide Werte sind also sehr eng aneinander gekoppelt. Durch die kognitive Komponente der Sicherheit gilt dies sogar in recht scharfer Weise. Denn Freiheit ist damit selbst eine stark kognitiv bedingte Größe und entsprechend leicht störbar. In einem Satz: Frei ist, wer sich frei fühlt. Nur dann „traut" man sich auch, frei zu handeln. Dadurch ist Freiheit also unter Umständen sogar recht leicht störbar und zerstörbar.

K

Kontrollaufgabe 2.6: Sicherheit und Freiheit

Was ist der Zusammenhang von Sicherheit und Freiheit? Wie kann man ihren Konflikt formulieren? Auf welche Weise ist er notwendig?

2.6 Freiheit in der Informationsethik

Mit diesen Vorbemerkungen können wir uns nun in den Bereich der „digitalen Freiheiten" wagen, also jener Freiheiten, die im Kontext der Informationstechnik und der in diesem Sinne technisch befassten Informationsethik eine besondere Rolle spielen, um dann pro Freiheit zu überlegen, ob und wie Einschränkungen durch Sicherheit legitim sein können. Hier müssen vor allem drei Themenkreise besprochen werden. Zuerst sollen die konkreteren Freiheiten in drei Varianten digitalen Handelns besprochen werden: dem Bezug sowie dem Austausch von Information und Wissen, dem Bezug digitaler Güter und der allgemeinen Kommunikation One-To-One oder One-To-Many. Schließlich muss der Bezug der hier anfallenden Freiheiten zu den Menschenrechten angesprochen werden, denn die hier existierende, direkte Verbindung macht die digitalen Freiheiten besonders wichtig und ihren Erhalt besonders drängend.

2.6.1 Information als Menschenrecht

Zuerst wollen wir uns ein wichtiges Korrelat für die folgenden Überlegungen ansehen – die Menschenrechte. Warum spielen die Menschenrechte hier eine Rolle? Freiheiten werden seit dem Zweiten Weltkrieg vor allem über die Menschenrechte definiert. Natürlich sind diese eher grobe Richtlinien und keine bindenden Rechte, die sich real juristisch und nicht nur

politisch einklagen lassen. Aber in den meisten „westlichen“ Staaten bilden sie den Hintergrund für die entsprechenden nationalen Gesetzgebungen auf Grundrechtsniveau. Dies liegt daran, dass sie für diese Form von Rechtskulturen grundlegende Überzeugungen aussprechen. Die Kernwerte dieser Überzeugung sind Freiheit, Gleichheit und Gerechtigkeit. Freiheit und Gerechtigkeit sind dabei Kernwerte, die dauerhafte Konstanten fast aller Gesellschaften sind. Im Falle der Freiheit haben wir das bereits ansatzweise diskutiert. Freiheit als Gegenkorrelat von Sicherheit gibt die Menge der selbst steuerbaren Handlungen vor, wobei allerdings verschiedene Gesellschaften unterschiedliche Rahmenbedingungen und Ausdehnungen dafür festmachen, die im Extremfall totalitärer Herrschaft entsprechend eng sind. Gerechtigkeit ist etwas anders gelagert, spielt aber ebenfalls eine wichtige und universale Rolle. Sie ist vorrangig ein Prinzip der Rechtsprechung, das jedem Teilnehmer einer Gesellschaft ein dem jeweiligen gesellschaftlichen Vertrag angemessenes Maß an Ausgleich bei absichtlich zugefügten Schäden oder entsprechend Strafen bei der Zuführung von Schäden zusichert. Gerechtigkeit ist in dieser Form ein zwingender Bestandteil eines funktionierenden oder überhaupt irgendwie gültigen Gesellschaftsvertrags. Allerdings gilt Gerechtigkeit in einem Staat nicht nur streng rechtlich bei konkreten Schadensfällen. Sie gilt auch in einem weiteren, politischen Sinn. Eine Gesellschaft muss das Gefühl haben, nicht nur in Streitfällen gerecht beurteilt zu werden, sondern auch gerecht Möglichkeiten der Lebensentfaltung zu haben. Was bedeutet das? Dieses Empfinden bezieht sich vor allem auf die gerechte Verteilung von Möglichkeiten der Lebensgestaltung und Mitteln. Sind bestimmte Lebenswege kategorisch nur für bestimmte Gesellschaftsgruppen zugänglich und nicht für andere, so wird dies als ungerecht empfunden – und stellt übrigens im Weiteren damit auch ein nicht unerhebliches Sicherheitsrisiko dar. Ungerechtigkeiten sind in aller Regel einer der zuverlässigsten „Brandbeschleuniger“ gewaltsamer Umstürze. Das soll aber nur nebenbei erwähnt sein. Ungerecht ist also, wenn einige wenige etwas dürfen und können, was andere nicht dürfen und können. In dieser – im Übrigen völlig subjektiven und rational nur schlecht eindeutig zu rekonstruierenden – emotionalen Haltung gibt es nun aber verschiedene Möglichkeiten für Ausnahmen und Ausdehnungen. Einer der wesentlichsten Unterschiede im Empfinden hat die Welt fast ein Jahrhundert in großer Spannung gehalten und hatte das Potential, eine völlige Auslöschung der Menschheit zu provozieren. Daran sieht man übrigens schon, dass solche subjektiven Empfindungen und der Umstand der Unmöglichkeit der logischen Auflösung alles andere als trivial sind. Die Rede ist von der Gerechtigkeit der Verteilung der deutlich verbesserten und

verbreiterten Basis der Mittel und den mit dieser Verteilung einhergehenden möglichen Verbesserungen der Lebensqualität zu Beginn der echten Wirkung der Industrialisierung. In dieser Zeit nämlich wurde klar, dass materieller Reichtum und damit einhergehend Macht und Lebensqualität produziert würden. Wie also sollte das verteilt werden? Dazu gab es dann in der Folge – sozusagen in der „Selbstfindungsphase" der neuen, industrialisierten Menschheit – zwei Möglichkeiten. Die erste war die der Sozialisten und Kommunisten. Der gesteigerte Reichtum sollte allen einigermaßen gleichmäßig zur Verfügung gestellt werden. Die zweite Möglichkeit war die der Kapitalisten. Der gesteigerte Reichtum sollte proportional zur Leistung, zum Beitrag zu diesem Reichtum verteilt werden. Es gab für beide Seiten eine lange Reihe guter und wichtiger Argumente. Aber das große Problem bei diesen beiden Ideen war, dass beide gerecht sind, sich aber trotzdem gegenseitig ausschlossen. Das Gerechtigkeitsempfinden entstammt dabei dem ganz alltäglichen Empfinden solcher Umstände und korreliert zur Zuordnung der Urheberschaft des Reichtums. Die Sozialisten und Kommunisten werten den gesteigerten Reichtum als Ergebnis eines gemeinsamen, gesellschaftlichen Aufwands in Erfindung und Realisierung. Der Urheber sind also „alle", und wenn alle etwas erstellen, ist es eben gerecht, dass alle etwas davon bekommen. Die Kapitalisten dagegen identifizieren den Ursprung des Fortschritts vor allem im Erfinder-Entrepreneur. Damals war das noch eine sehr typische Kategorie von Industrialist. De facto leistet der Erfinder-Entrepreneur „mehr" für den Fortschritt der Industrialisierung. Ohne ihn und seine Risikobereitschaft, seinen Erfindungsreichtum und seine Führungsfähigkeiten gäbe es die Industrialisierung nicht. Der Urheber ist also ein bestimmter Typ von gesellschaftlichem Akteur, zumindest etwas mehr als andere, und hier greift ein anderes Gerechtigkeitsprinzip unseres Alltags: Wer mehr tut, bekommt auch mehr. Auch dies ist nur gerecht. Jemand, der in einer Gemeinschaft keine Lust hat, etwas beizutragen, wird in der Regel von dieser Gemeinschaft nicht noch umfangreich mit Gütern ausgestattet. Dies würden sogar jene, die hart arbeiten und viel beitragen, wieder als ungerecht empfinden – erneut mit den entsprechenden Risiken für die allgemeine Sicherheit.

Beide Verteilungsvarianten sind also gleichzeitig gerecht und ungerecht. Eine Krux unseres sozialen Empfindens, die in ähnlicher Form auch bei vielen anderen Gelegenheiten wieder erscheint. Wie entscheidet man nun, welche man umsetzen möchte? Traditionell geht die Menschheit in solchen Situationen auf das Schlachtfeld und trägt die Angelegenheit mit Fäusten und anderen Dingen aus. In der causa Kommunismus vs. Kapitalismus

wäre es auch bestimmt so weit gekommen, wären nicht zu jenem Zeitpunkt die Atombomben erfunden worden, die aufgrund der zu erwartenden immens hohen Verluste die Entscheidung über neue Verteilungsformen haben weniger wichtig aussehen lassen. Das Ergebnis ist aus dieser Perspektive interessant. Statt den Wert eines Wirtschaftssystems mit den Fäusten auszutragen, bekamen beide Systeme die Chance, sich zu bewähren. Den Verlierer kennen wir inzwischen. Es kann mit Recht gemutmaßt werden, ob es wirklich allein das Wirtschaftssystem war, das den Untergang der Sowjetunion, des bislang größten politischen Realexperiments, bewirkt hat, und ob nicht Kalter Krieg und die Konkurrenzsituation zu den USA auch einen erheblichen Anteil hatten. Sicher lässt sich aber sagen, dass die äußerst geringe Freiheit, deren Einschränkung durch die Erfordernisse der industriellen Umstellung der des latenten Konflikts für notwendig erachtet wurde, einen wesentlichen Anteil am Untergang des Systems hatte.

Ein weiterer Bestandteil des Untergangs war dann aber auch das letzte Konstitutivum unserer Menschenrechte – die Gleichheit. Für die kommunistischen Staaten gab es damals eine Redewendung, die oft mit einigem Zorn vorgetragen wurde: Alle sind gleich, aber einige sind gleicher. Damit wurde der Umstand ausgedrückt, dass zwar der Ideologie gemäß alle Bürger vollkommen gleich waren, im konkreten System allerdings die politisch oberen Klassen deutlich mehr Freiheiten und Vorzüge genossen, also von der Gleichheit im Grunde ausgeschlossen waren und das realisierten, was sie eigentlich abschaffen wollten - Ungleichheit in der Behandlung von Menschen. Dies ist eine Beobachtung, die sich in vielen Gesellschaften in unterschiedlicher Form machen lässt. Gerechtigkeit bedingt Gleichheit, aber es kann gesetzlich, also in konkreten Ausformulierungen des Prinzips, die Möglichkeit der Ausnahme bestimmter Gruppen unter bestimmten Umständen festgehalten werden. Dies gilt häufig natürlich für die führenden Gremien einer Gesellschaft, die in der Macht stehen, solche Ungleichheiten zu ihren Gunsten aufzustellen. Es kann aber auch für Gruppen gelten, die aufgrund informeller Merkmale besser aufgestellt ist. So ist es in den modernen westlichen Welten oft so, dass Reiche weit weniger hart bestraft werden als Arme, bei sonst gleichen Sachständen. Dies liegt dann einfach daran, dass sie sich mit ihrem Geld bessere (oder überhaupt) Anwälte leisten können, die ihre Interessen vor Gericht vertreten. In dieser Hinsicht sind also Systeme formell und informell formbar und lassen Ungleichheiten zu. Dennoch sind die Gleichheiten in den modernen westlichen Staaten am deutlichsten ausgeprägt im realen Leben und am ausführlichsten formuliert. Dies liegt eben an der engen Bindung der westlichen Gesellschaften an die

Menschenrechte und an deren expliziter Formulierung einer universalen Geltung von Gleichheit für alle Menschen, ganz gleich, welcher Herkunft, welcher Religion, welchem Geschlecht oder welchem anderen Merkmal sie sonst angehören. Diese deutliche Bezugnahme wurde im Gefolge des Zweiten Weltkrieges und dem durch den Holocaust entstandenen Worst Case einer Ungleichheit beschlossen.

Neben diesen allgemeinen und übergreifenden Prinzipien gibt es eine Reihe von Bedingungen, von denen man annimmt, dass sie politisch herrschen müssen, um diese Prinzipien in der Variante der Menschenrechte entsprechend universal zu realisieren. Wichtig sind etwa die Bedingungen der Rechtsstaatlichkeit und der Demokratie. Nur unter diesen juristischen und politischen Rahmenbedingungen – so zumindest argumentiert ein größerer Kanon demokratischer Politiktheoretiker – können universale Menschenrechte real eingeführt und durchgehalten werden, in gültige Grundgesetze überführt werden, deren Befolgung gegen jeden und unter jeden Umständen einklagbar wird. Regierungen müssen wählbar und vor allem abwählbar sein, damit sie keine Ungerechtigkeiten und Unfreiheiten dauerhaft einführen können. Rechte und Rechtsmodifikationen durch Regierungen müssen einklagbar sein, um Gerechtigkeit und Gleichheit zu garantieren.

Innerhalb dieses Rahmens sind dann auch einige weitere Freiheiten zu garantieren, die eine funktionierende rechtsstaatliche Demokratie überhaupt ermöglichen. Dazu gehört nun wesentlich auch das Recht auf Information. Der Zusammenhang wird leicht klar. Ohne klare Informationen über die Handlungen der Regierung und anderer Institutionen wie der Wirtschaft kann nicht klar über deren Konformität mit den Prinzipien des Menschenrechts geurteilt werden. Indem also der Zugang zu Information und natürlich auch der Austausch von Information in Kommunikation eine condicio sine qua non von Demokratie und Rechtsstaat sind und indem Demokratie und Rechtsstaat condiciones sine qua non der Menschenrechte sind (oder zumindest der Theorie nach die besten möglichen Organisationsformen zu deren Garantie), werden transitiv rückwirkend die Freiheiten zur Information selbst zum Menschenrecht. Davon ausgehend lassen sie sich nun in verschiedenen Versionen in Menschen- und Grundrechten wiederfinden.

2.6.2 Freiheit (des Bezugs, des Bereitstellens und des Austauschs, der Kommunikation) von Information

Die wichtigste Anwendung der Informationsfreiheit findet sich im Bezug, im Bereitstellen und im Austausch, in der Kommunikation von Informati-

on in der Form einzelner Fakten oder größerer Wissenszusammenhänge und Meinungen. Dies ist die allgemeine Meinungsfreiheit, in den USA auch als „freedom of speech“ bezeichnet, die durch die Wissensfreiheit, die Informationsfreiheit und die Pressefreiheit ergänzt wird. Dabei ist die Meinungsfreiheit der Garant für eine freie Bildung und Vertretung einer Meinung, die Wissensfreiheit der Garant dafür, dass man sich durch freien Zugang zu Information jede Form von Wissen aneignen darf, um eine Meinung zu bilden, die Informationsfreiheit ein Bürgerrecht auf Einsicht in öffentlich relevante Dokumente und Prozesse und die Pressefreiheit eine formale Freiheit der Presse, Fakten einzuholen und Wissen von Gefährdungen abgesehen uneingeschränkt zu produzieren.

Hier einige Definitionen dieser Freiheiten:

D

Definition 2.2: Beispiele für Beschreibungen und Definition der Meinungsfreiheit und assoziierter Freiheiten

Im Rahmen der UN ist die Meinungsfreiheit in Art. 19 der Universal Declaration of Human Rights ausformuliert:
„Jeder Mensch hat das Recht auf freie Meinungsäußerung; dieses Recht umfasst die Freiheit, Meinungen unangefochten anzuhängen und Informationen und Ideen mit allen Verständigungsmitteln ohne Rücksicht auf Grenzen zu suchen, zu empfangen und zu verbreiten.“

In Deutschland sind Meinungsfreiheit und Pressefreiheit im Artikel 5, Grundgesetz festgehalten:
„(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.
(2) Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.“

Die Wissensfreiheit ist in Deutschland im gleichen Artikel 5, Absatz 3 definiert:
„Die (3) Kunst und Wissenschaft, Forschung und Lehre sind frei. Die Freiheit der Lehre entbindet nicht von der Treue zur Verfassung.“

In den USA ist die „Freedom of Speech“ im First Amendment der Bill of Rights festgehalten:
„Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.“

Nun ist allerdings klar, dass diese Formulierungen nicht im Hinblick auf das Internet und die damit zusammenhängenden neuen Modalitäten der Verbreitung und des Bezugs von Informationen gefasst wurden. Das Internet modifiziert klassische Informations- und Kommunikationshandlungen vor allem dadurch, dass es sie wesentlich leichter macht und dass sie es jedem Teilnehmer ermöglicht, Sender von Informationen an viele weitere Rezipienten zu sein. Positiv daran ist, dass damit eine wesentlich breitere politische Bildung und ein umfassenderer politischer Diskurs stattfinden können. Als weiterer Vorteil wurde häufig genannt, dass das Internet auch nicht durch „die Mächtigen“ kontrolliert werden könne, dass also ein in hohem Maße herrschaftsfreier Diskurs stattfinden kann. Dieser Eindruck ist temporär durch die Rolle des Internets in der Koordinierung des Aufstands im Arabischen Frühling entstanden. Allerdings ist das ein äußerst fehlerhafter Eindruck, denn de facto ist das Internet – und dies sind zwei wichtige negative Momente in der Anwendung der Informationsfreiheit auf das Internet – (a) manipulierbar und mit ausreichenden Ressourcen auch (b) kontrollierbar und zumindest in den Kommunikationsakten technischer Laien personalisierbar. So ist also bei dort stattfindender Kommunikation nie eindeutig klar, wer mit welchen Absichten welches Wissen kommuniziert und ob die Informationen ausreichend zuverlässig und wahr sind. Diese freie Manipulierbarkeit ist in der Struktur des Internets, insbesondere in den aus Sicht eines eigentlich wünschenswerten herrschaftsfreien Diskurses positiv relevanten Merkmalen der Möglichkeit der Anonymität und der Pseudonymität angelegt.

Diese und einige weitere Möglichkeiten und Bedingungen des Internets bilden nun die besondere Herausforderung an eine Anwendung der Menschenrechte, insbesondere der Rechte der freien Meinung und der freien Information. Diese Anwendungen müssen darauf abzielen, die Bedeutung der neuen Technologien als Enabler eines besseren und unabhängigen politischen Diskurses herauszustellen und sie in dieser Form rechtlich zu sichern, insbesondere gegen die negativen Potentiale der Technologie.

Dieser Prozess ist noch nicht sehr lange in Bewegung und negiert im Moment zumindest noch die negativen Momente der Informationstechnologien. Ein Grund dafür ist, dass der politische Diskurs vorrangig von Technikoptimisten geführt wird, die eine Realisierung der positiven Momente der der nachteiligen Momente politisch deutlich bevorzugen. Dies ist eine naive und unverantwortliche Haltung, andererseits aber normaler politischer Prozess.

Einige Debatten und Festlegungen haben allerdings bereits stattgefunden. Eine erste Erklärung, das „Statement on Human Rights, Human Dignity and the Information Society“, das im November 2003 kurz vor dem ersten World Summit on Information Society („WSIS“, Dezember 2003) abgegeben wurde und das später im Rahmen der Konferenz noch von einer Erklärung der Zivilgesellschaft mit Bezug zu den Menschenrechten flankiert wurde („WSIS I“), identifizierte eine umfassende Liste von Rechten, die unmittelbar mit der digitalen Freiheit des Ausdrucks und der Information zu tun haben. Darunter finden sich Rechte wie:

- Right to participate in public affairs – durch den Bezug und den Austausch politischer Informationen und Meinungen;
- Right to education – durch den Bezug aller Arten von Wissen und Meinungen
- Right to reply – als Antwort auf digitale Fragen oder Beschuldigungen
- Right to fair administration of justice – etwa insofern als hier auch der Bezug von juristischem und sachdienlichem Wissen eine Rolle spielen kann oder indem eine Kommunikation mit einem Anwalt online stattfinden und dann vertraulich behandelt werden kann
- Right to participate in cultural life – etwa insofern als viel kulturelles Leben online in Form von Informationen stattfindet
- Right to health – etwa insofern als Informationen über medizinische Behandlungen und gesunde Ernährungen online bezogen werden können
- Right to an adequate standard of living & right to adequate housing – etwa insofern Informationen über Produkte und Wohnungen online beschafft werden können

Einige weitere Rechte wie inklusionsbezogene und Privatheitsrechte wurden ebenfalls identifiziert und werden weiter unten noch besprochen.

In den konkreten Ausführungen dieser Freiheiten sind allerdings Einschränkungen möglich. Einschränkungen sind im Menschenrecht immer dann möglich, wenn andere Menschenrechte betroffen sind. Dies ist auch im Bezug auf die Bewegung von Informationen möglich. Drei Beispiele wollen wir betrachten.

- Verbot der Beleididung
  Ein anderes Menschenrecht ist das auf eine eigene Persönlichkeit und auf die respektvolle Behandlung dieser Persönlichkeit. Im bundesdeutschen Recht wird dies auch als das „Allgemeine Persönlichkeitsrecht“ bezeichnet. Dieses Recht kann durch Beleidigungen einschränkt werden, wobei Beleidigungen gleichzeitig keine notwendige Form einer politischen Kommunikation sein müssen. Daher kann die Meinungsfreiheit eingeschränkt werden, wenn es sich um persönliche Beleidigungen handelt. Diese sind mitunter rechtlich anklagbar und verboten.

- Verbot menschenrechtsverachtender Meinung
  In Deutschland gilt es aufgrund unserer Geschichte im Kontext des §130, Absatz 4 des Strafgesetzbuches als verboten und mit Freiheitsstrafe bedroht, wenn jemand „öffentlich oder in einer Versammlung den öffentlichen Frieden in einer die Würde der Opfer verletzenden Weise dadurch stört, dass er die nationalsozialistische Gewalt- und Willkürherrschaft billigt, verherrlicht oder rechtfertigt.“ Diese Einschränkung der Meinungsfreiheit betrifft auch Medien, indem etwa rechtsradikale Medien in Print und Online verboten und eingeschränkt werden können.

- Verbot der Verbreitung gefährlichen Wissens
  In vielen Ländern gilt es außerdem als verboten, Wissen zur Verfügung zu stellen, das Gefahren für Leib und Leben produzieren kann. Darunter fallen etwa Anleitungen zum Bombenbau.

2.6.3 Inklusion und Nicht-Diskriminierung

Ein weiteres wichtiges Element ist das der Inklusion und Nicht-Diskriminierung. Damit ist gemeint, dass alle Menschen gleichen Zugang zu den neuen Möglichkeiten der Bewegung von Information erhalten sollten, um keine Benachteiligungen durch mangelnde Informationen oder

mangelnde Geschwindigkeiten im Bezug von Informationen entstehen zu lassen. Als besonders zu berücksichtigende Rechte gelten dabei nach dem bereits erwähnten Dekalarationstext WSIS I:

- Women's rights
- Gender equalities
- Rights of minorities
- Workers' rights
- Rights of indigenous people
- Rights of the child
- Rights of persons with disabilities

2.6.4 Freiheit des Bezugs digitaler Kultur

Neben diesen immer noch stärker auf die Informationsfreiheit abgestellten Freiheiten lassen sich noch weitere ausmachen. Eine Freiheit ist durch das Recht an der Teilnahme an einem kulturellen Leben ausgedrückt. Auch dies ist eines der Rechte des Katalogs der Menschenrechte („right to participate in cultural life"). Es betrifft das digitale Leben, da inzwischen eben viel kulturelles Leben online in verschiedenen Kommunikations- und Medienformen stattfindet. Diese besondere Variante war auch bereits einmal gesetzlich aktiviert, als Frankreich im Rahmen der Versuche einer Strafverfolgung gegen illegale Raubkopien von Medien („illegales Filesharing") in seiner HADOPI-Gesetzesvorlage vorschlug, Gesetzesverstöße im Internet mit dem Ausschluß vom Internet zu bestrafen. Sollten Personen dreimal bei einem Gesetzesverstoß erwischt werden, sollte ihnen die Teilnahme am Internet versagt bleiben (sog. „Three Strikes" Regel). Dieser Vorschlag hatte allerdings mit erheblichen Schwierigkeiten zu kämpfen, da eben mit solch einer Regelung der Bezug von Information erschwert und die Teilnahme am digitalen, kulturellen Leben verhindert wird.

Dieses Menschenrecht wurde nun allerdings insbesondere im Kontext der Diskussion um illegales Filesharing auch missbräuchlich interpretiert. Die Befürworter einer vorbehaltslossen Legalisierung illegalen Filesharings etwa nahmen das Argument in Anspruch, dass mit den Möglichkeiten des freien und vor allem schnellen und kostenlosen Bezugs von medialen Inhalten ein wesentlich angereichertes kulturelles Leben stattfände. Diese Argumente waren aber selbstredend nicht ausreichend stichhaltig – wie

auch alle anderen Argumente der Befürworter dieser Praxis – da hier das einfache und grundlegendere Gerechtigkeitsprinzip der angemessenen Entlohnung von Arbeit verletzt wird. Durch das illegale Filesharing wird in die Freiheit der Produzenten eingegriffen, selbst ihre Produkte vertreiben zu können und dafür eine Entlohnung einzufordern. Der Rekurs auf den Menschenrechtsstatus kann dabei nicht unternommen werden, um einen hohen Wert des illegalen Sharings einzuklagen, da auch das Recht auf die Verwertung der eigenen intellektuellen Kreationen ein Menschenrecht im gleichen Rang ist („right to the protection of the moral and material rights over intellectual creations“).

2.6.5 Privatheit

Eine weitere wichtige Freiheit in diesem Kontext ist der Rückzug von Information im Privaten. Dieses besondere Recht – ebenfalls ein Menschenrecht – ist allerdings herausragend bedeutend für die Informationsethik und der Grundpfeiler des Datenschutzes, so dass wir die Privatheit in großer Detailschärfe im nächsten Studienbrief bearbeiten wollen.

2.6.6 Weitere relevante Freiheiten

Im Katalog der Menschenrechte sind noch einige weitere Freiheiten erwähnt, die ebenfalls für Informationsgesellschaft besonders relevant sind. Diese Liste ist recht extensiv, da Wissen und Information nun einmal recht grundlegende Elemente vieler Handlungen und damit auch vieler Freiheiten sind. Sie umfasst: Free

2.7 Zusammenfassung

Zu Beginn des Studienbriefs wurde die problematische Definition von Sicherheit im gesellschaftlichen Rahmen betrachtet. Dabei wurde auf die Ansichten von Thomas Hobbes näher eingegangen und als Grundlage für weitere Betrachtungen eingeführt. Anschließend wurde der Wert der Sicherheit dargelegt und anhand des Beispiels – dem Angst vor dem Tod – veranschaulicht. In dem Abschnitt 2.4 Prinzipien der Sicherheitsrationalität wurden die vier Prinzipien beschrieben und der Zusammenhang zu Handlung und Wahrnehmung von einzelnen Personen dargelegt.

In dem Abschnitt 2.5 Sicherheit und Freiheit wurde auf den Verhältnis zwischen Freiheit und Sicherheit eingegangen. Dabei reicht die Androhung von Strafe, um die Menschen vor Unfreiheit und somit vor Taten abzuhalten.

Des Weiteren wurde in Abschnitt 2.6 Freiheit in der Informationsethik auf die Information als Menschenrecht und der Freiheit von Informationen im Allgemeinen hergeleitet. Dabei wurde am Ende des Kapitels auf die Inklusion und Nicht-Diskriminierung sowie die Freiheit von Bezug digitaler Güter erwähnt.

2.8 Übungen

Übung 2.1

Ü

1. Wie bewerten Sie den Trade-Off zwischen Freiheit und Sicherheit?
2. Wo liegt Ihrer Meinung nach eine gute Mitte?
3. Wie lässt sich diese erreichen?

Übung 2.2

Ü

1. Welche weiteren Bedingungen und Prinzipien lassen sich zur Sicherheitsrationalität anführen?
2. Wie werden aus der Perspektive der Sicherheitsrationalität andere Wertrationalitäten wahrgenommen?
3. Wie wird eine Priorität von Freiheit wahrgenommen?

Studienbrief 3 Einführung in den Datenschutz

3.1 Lernziel

Was wird Ihnen vermittelt?

In diesem Studienbrief sollen ein Überblick über den Datenschutz gegeben werden. Dies umfasst die Kennzeichnung von öffentlichen Informationen, das Prinzip der informationellen Selbstbestimmung, einen Einblick in das Bundesdatenschutzgesetz und die Probleme der Handhabung dieses Gesetzes. Nach Beendigung dieses Studienbriefes soll ein grundlegendes Verständnis über den Datenschutzes und der Bedeutung für die Bürger vorherschen.

3.2 Advanced Organizer

Für den Studienbrief 3 Einführung in den Datenschutz sind keine Vorkenntnisse notwendig. Es werden grundlegende Prinzipien, Zusammenhänge und der Sinn des Datenschutzgesetzes erklärt, um die Historie und Notwendigkeit des Datenschutz zu verstehen.

3.3 Einführung – Öffentlich und Privat als Kennzeichnung von Information

Privatheit ist ein altes Gut der Menschheit. Über ihre historische Entstehung lässt sich viel spekulieren. Foucault etwa verortet sie im frühen Bürgertum und erachtet den Vorhang bereits als ein erstes, wichtiges technisches Werkzeug zur Erreichung von Privatheit.

Wie Sicherheit kann Privatheit gut ex negativo erfasst werden. Denn so wie Sicherheit die Abwesenheit von Gefahr adressiert, wird Privatheit durch eine spezifische Abwesenheit von Informationen umrissen, nämlich durch die Abwesenheit „privater" Informationen im öffentlichen Informationsraum. Damit wird einer Trennung zweier Lebensräume entsprochen. Der öffentliche Raum ist der Raum der Gemeinschaft, in dem Politik und die Gemeinschaft betreffende Themen, aber auch die Gemeinschaft betreffende Rechte und Pflichten besprochen, adressiert und durchgesetzt werden. Dazu müssen Informationen von den Teilnehmern der Gesellschaft zur Verfügung gestellt werden, die, indem sie die Gesellschaft als Ganzes betreffen, eben nicht allein Sache der Teilnehmer sind, sondern Sache der Gemeinschaft.

Bereistellung von Daten für die Öffentlichkeit

B

Beispiel 3.1: Steuern

Das beste Beispiel sind steuerrelevante Informationen. Die Gemeinschaft leistet für den Einzelnen eine Reihe von Diensten (darunter etwa den Datenschutz und die Sicherheit), wofür der Einzelne eben Steuer entrichten muss. Die Steuer ist in ihrer Höhe in den meisten Fällen relativ zu den Einnahmen ausgerichtet. Damit sind also die Informationen über Einnahmen eine öffentliche Angelegenheit, da so die Öffentlichkeit bestimmt, was ihr zusteht.

Private Daten

Anders dagegen sieht es aus mit Informationen etwa über eine Freundschaft. Dies ist normalerweise etwas, das rein dem privaten Raum zuzurechnen ist. Wer mit wem auf welcher Basis und in welchem Grad von Intimität befreundet ist, betrifft die Öffentlichkeit normalerweise in keiner Weise (sofern damit keine gesellschaftsschädlichen Folgen verbunden sind), so dass hier also keine Pflicht der Information der Öffentlichkeit besteht. Diese Informationen sind „privat". Öffentlichkeit und Staat haben kein Anrecht auf sie. Über ihre Distribution entscheidet im Idealfall allein die Einzelperson. Eine weitere Verschärfung dieser Privatheit und ein gewissermaßen genuiner Bereich des Privaten finden sich noch in Bereichen, die als „intim"

Intimität

empfunden werden. Sexuelle Praktiken sind hier als ein verständliches Beispiel zu nennen. Hier ist nun das Empfinden von Privatheit besonders stark ausgebildet. Man möchte in der Regel, dass nur ein sehr eng umrissener und gut kontrollierbarer Personenkreis von diesen Dingen weiß.

Fließende Abgrenzungen

Allerdings gibt es für die Abgrenzungen der privaten und der öffentlichen Räume keine festen und ewigen Linien. Diese Verhältnisse sind eher dauernd im Fluss. Sie können manchmal mehrere Jahrhunderte halten, können dann aber aufgrund veränderter gesellschaftlicher Verhältnisse und Wertungen innerhalb weniger Generationen verworfen und neu ausgerichtet werden.

B

Beispiel 3.2: Kindeserziehung

Ein Beispiel für einen solchen Gegenstand des Privaten ist die Erziehung von Kindern. Sie galt viele Jahrhunderte als reine Privatangelegenheit, wurde aber in den letzten Jahrzehnten in einigen Kulturen in die Öffentlichkeit gebracht und wird heute als nicht vollständig aber in vielen Beziehungen öffentliche Angelegenheit betrachtet. Körperliches Strafen oder die Sprachentwicklung beim Kind etwa sind Elemente, die früher privat waren, heute aber als durch die Gemeinschaft korrigierbar und steuerbar gelten. Hier gab es unter anderem einen Wandel durch die Erfahrungen der beiden Weltkriege, in deren Nachgang man eine andere kulturelle Menschwerdung anstreben wollte als die „traditionelle“, die eine entsprechende hohe Toleranz, wenn nicht Wertschätzung für den Krieg oder mindestens den bürgerlichen Gehorsamkeitsethos mit sich brachten, die in Folge der Weltkriege als zu gefährliche menschliche Haltungen erachtet wurden und entsprechend eine Einmischung der Öffentlichkeit in das vormals private, abgeschlossene Reich der Kindeserziehung notwendig machte.

Aber nicht nur historisch gibt es Veränderungen im Empfinden von Privatheit, auch verorten verschiedene Kulturen das Private und das Öffentliche je anders. So gibt es immer wieder verschiedene Gesellschaften, die etwa verschiedene Bereiche des Sexuellen in den Bereich des Öffentlichen ziehen und die zum Beispiel Homosexualität als gemeinschaftsschädigend empfinden und entsprechend identifizieren und regulieren wollen.

Bedeutung von Privatheit

Das Private von heute muss also nicht das Private von morgen und auch nicht das Private unserer Nachbarn sein. De facto muss man Gesellschaften

eine Flexibilität in der Aushandlung dieser Werträume zugestehen, denn so können sie sich besser auf neue Herausforderungen und Probleme einrichten und anders agieren. Allerdings – das Beispiel der Homosexualität indiziert dies – sind häufig auch grundlegende Menschenrechte wie das Recht der Gleichheit vor dem Gesetz mittelbar von Einschränkungen der Privatheit betroffen. In diesen Fällen muss man folglich strenger hinsehen und anders urteilen. Dabei kann eine Reihe von Menschenrechten von Privatheitsverlusten intensiv betroffen sein. Jedes Recht schützt einen Lebensaspekt, und jeder Lebensaspekt kann sofort eingeschränkt sein, wenn er öffentlich wenig toleriert wird und wenn Informationen über ihn öffentlich werden. Privatheit schützt also auch Menschenrechte über den Schutz der Informationskomponente jedes Menschenrechts und ist nicht allein, aber auch infolge dessen ein Menschenrecht.

Für die Bestimmung des Privaten und des Umgangs mit privaten Informationen sind nun allerdings nicht nur die Grenzen der beiden Räume konstitutiv. Wir können das Beispiel der Steuereinnahmen wieder heranziehen. Dabei ist nun zu beachten, dass die Relation noch etwas spezifischer ausgestaltet ist. Die Informationen über steuerrelevante Einnahmen sind relevant für die Öffenltichkeit, aber die Einnahmen einer Person gehen selbstredend nicht jeden in einer Gemeinschaft etwas an. Müsste man sich jedem gegenüber öffnen, könnten etwa Kriminelle mitlesen und auf diese Weise Ziele für ihre Machenschaften identifizieren. Es dürfen also nicht alle Teilnehmer einer Gesellschaft diese „öffentlichen“ Informationen einsehen, sondern nur diejenigen institutionellen Vertrauenspersonen, die dafür spezifisch abgestellt, rechtlich reguliert und verantwortlich sind. Damit offenbart sich eine weitere wichtige Relation der Privatheit. Neben der Trennung von öffentlich und privat gibt es eine Reihe genauerer Informationsverhältnisse, die Typen von Rezipienten, Inhalte von Informationen und Wege der Vermittlung genauer regeln. In diesem Bereich greifen nun eine Reihe verschiedener Gesetze, die erst mit Aufkommen der digitalen Technologien auch als Datenschutzgesetze verstanden und kategorisiert werden, aber selbstredend schon vorher existiert haben.

Informationsflussregelung

Das Private ist also Raum des Agierens und Seins, der der Gemeinschaft nicht zugänglich oder nur unter bestimmten Umständen und in bestimmten Formen zugänglich sein sollte. Das Öffentliche dagegen als Gegenstück ist ein Raum des Agierens und Seins, der die Öffentlichkeit in verschiedenen Weisen betrifft, für den sie zuständig ist, und zu dessen Bearbeitung Informationen zugänglich gemacht werden müssen. Dabei sind „privat“

und „öffentlich“ beides Begriffe, die vorrangig über Information verstanden werden können, indem eben in beiden Fällen eine bestimmte Variante von Informiertheit und Information (als Akt) kennzeichnend für die Zuordnung eines bestimmten Begriffs in Abgrenzung zum anderen ist.

3.4 The Right To Be Left Alone

Bevor wir nun im folgenden enger auf die informationelle Privatheit, also den spezifischen Aspekt der Information im Kontext von Privatheit eingehen, wollen wir uns noch mit einem wichtigen Aufsatz aus der Vergangenheit der Privatheit beschäftigen. Er wurde 1890 von den beiden US-amerikanischen Rechtstheoretikern Warren und Brandeis verfasst und skizziert Privatheit im Allgemeinen nach dem Ausspruch eines noch früheren Richters Judge Cooley „right to be left alone“. Warum wurde der Aufsatz wichtig für die Datenschutzdiskussion? Die Intention von Warren und Brandeis war es zumindest erst einmal nicht, denn der Grund ihrer Beschäftigung ist ein Feldzug gegen die Regenbogenpresse. Die dort verbreiteten Trivialitäten bewerten die Autoren als schlecht für die menschliche Natur und Entwicklung. „Even gossip [...]“, so das Papier, „[...] is potent for evil.“ (36, S. 196) Und „Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence“ (36, S. 196). Diese Motive also führen Warren und Brandeis ins Feld. Sie möchten das private Leben anderer Personen nicht in der Öffentlichkeit diskutiert sehen. Das selbst wäre jetzt keine besonders bemerkenswerte Aussage, interessanter allerdings ist der Umstand, warum sie eine ausufernde Regenbogenpresse überhaupt als Problem erachten. Diese ist nämlich so umfangreich und lästerlich geworden durch einen technischen Fortschritt, der eine neuartige Invasion des Privaten begünstigte: „Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that, what is whispered in the closet shall be proclaimed from the house-tops.“ (36, S. 195). Dies, so die Autoren, sei ein Umstand, der vom Gesetz noch nicht erfasst sei und der eine Neuauflage der gesetzlichen Gedanken zu Privatheit notwendig machte.

Privatheit ist nämlich in den USA im 4th Amendement festgehalten. Dieses Amendement beschreibt im Grunde ein uraltes Gesetz des Common Law: „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be viola-

ted, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.“ (13) In alten Zeiten, so Warren und Brandeis, ist dieser Zusatz sehr wörtlich ausgelegt worden. Es ging um reale physische Bedrohung eines örtlich fest umrissenen Raumes. Indem nun aber neue Technologien neue Arten der Bedrohung andersartig umrissener privater Räume ermöglichen, müsse eine Erweiterung oder zumindest eine erweiterte Auslegung des Gesetzes erwogen werden. Mit Regenbogen-Presseberichten etwa würden zwar keine privaten Räume verletzt und keine realen physischen Verletzungen von Menschen stattfinden, aber die im Prinzip des privaten Raumes angelegte Idee, dass jeder selbst entscheiden kann „to what extent his thoughts, sentiments, and emotions shall be communicated to others“ (36, S. 193) wird durch die Möglichkeiten der Fotografie und die Geschäftsmodelle der neuen Zeitungen untergraben. Fotos greifen die Privatheit der Menschen in verschiedensten Räumen an, und eine Presseberichterstattung auf der Basis von Gerüchten und Vermutungen richtet dann Schaden an – keinen real-physischen Verletzungen, aber Verletzungen der Ehre und „mental suffering“.

Verletzung der Privatsphäre

An dieser Stelle liefert der Text also eine ideale Grundlage für die Betrachtung des Datenschutzes in unserer Zeit – und sogar für weitere und wiederholte Betrachtungen unter sich wieder verändernden Zeiten. Die Basislektion lautet, dass man sich der Intentionen der die Einzelpersonen in ihrer Privatheit schützenden Gesetze und Absprachen bewusst sein muss und diese Absichten auch unter sich verändernden technischen und gesellschaftlichen Bedingungen erhalten muss. Es muss also klar sein, was damit beabsichtigt war, was geschützt werden sollte und wie sich dieses Schutzgut unter neuen Bedingungen neu darstellt. Das ist exakt die Aufgabe des Datenschutzes.

Im Kontext der Privatheit geht es dabei vor allem um einen Schutz des intimen, eigenen Lebens (wie oben zitiert) vor dem öffentlichen Leben, der (nach Warren und Brandeis) niederen Neugier und dem Urteil über Lebensaspekte, deren Beurteilung allein den Betroffenen zusteht.

Dies wird von Warren und Brandeis schließlich auch genau so festgehalten: „[…] the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not

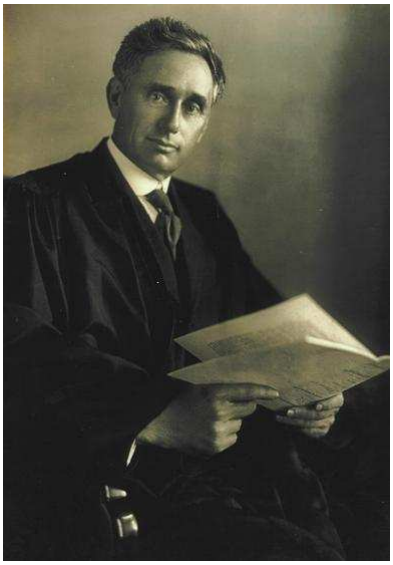


Abb. 3.1: Judge Louis Brandeis.

Quelle: http://www.acslaw.org/files/Brandeis.JPG

be assaulted or beaten, the right not be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed – and (as that is the distinguishing attribute of property) there may some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality." (36, S. 205)

Verfahren zur Telefonüberwachung

Louis Brandeis war in dieser Hinsicht später auch praktisch wegweisend, nicht nur theoretisch. Er saß nämlich 1928 als Richter in dem Fall „Olmstead vs United States" einem der ersten Fälle von Telefonüberwachung vor. Damals wollte die Polizei einen Ring von Alkoholschmugglern auffliegen lassen und klemmte sich an die öffentlich zugänglichen Telefonkabel, um deren Gespräche mithören zu können und sich entsprechend Zugang zu kritischen Informationen zu beschaffen. Im Gerichtsfall später beriefen sich allerdings die Beschuldigten auf das 4th Amendment, das den Schutz der Privatsphäre in den USA gewährleistet.

Die Polizei hätte nach Interpretation der Verteidigung nicht ohne eine richterliche Befugnis, einen Warrant, in ihre Privatsphäre eindringen dürfen – in der Tat hatte die Polizei sich nämlich keinen Warrant besorgt. Dort war man eben in einer missverständlichen, wortgenauen Auslegung des 4th Amendements davon ausgegangen, dass man nur im Falle eines ech-

ten physischen Eingriffs in die räumliche Privatsphäre, also einer echten Hausdurchsuchung, einen solchen Warrant benötigt. Das reine Abhören der im öffentlichen Raum befindlichen Kabel dagegen stellte in ihren Augen keine Verletzung der Privaträume der Angeklagten dar, da diese Räume nie betreten wurden.

Allerdings urteilte Brandeis gegen diese auf den rein physischen Ort fokussierte Interpretation der Polizei, indem er eben eine private Kommunikation als ebenfalls dem privaten „Raum“ zugehörig empfand. Entsprechend, so Brandeis, müsse das 4th Amendement nicht im Wortlaut, sondern in seinem Sinn interpretiert werden und dieser Sinn schließt eine private Kommunikation mit ein, auch wenn das Kabel dieser Kommunikation im öffentlichen Raum liegt. Brandeis ließ folgend die Beweise der Polizei nicht gelten.

Datenschutz: Sinngemäße Auslegung

Warren und Brandeis liefern also eine wichtige Grundeinsicht für den Datenschutz. Er muss nicht in einem Wortlaut, sondern sinngemäß unter sich ändernden technologischen und gesellschaftlichen Bedingungen ausgelegt und angewandt. Allerdings geht es beim Schutz der Privatheit nicht allein um den von Warren und Brandeis identifizierten Verlust von persönlicher Initimität, es geht auch um die politische Handlungsfähigkeit der Bürger in einer Demokratie. Dies ist ein Aspekt, den wir jetzt in Kürze im nächsten Abschnitt genauer bearbeiten wollen.

Abschließend zu Warren und Brandeis soll aber noch auf einen wichtigen Aspekt ihrer frühen Behandlung der Privatheit eingegangen werden, der in der Literatur weniger Beachtung gefunden hat, der inzwischen aber ebenfalls zusehends wichtig wird. Die Autoren hatten nämlich nicht nur die neue Technologie der Kamera, sondern auch die neuen Geschäftsmodelle der Zeitungen in ihrer Anklage adressiert. Dies ist etwas, das sich zwar in vielen konkreten Applikationen von Datenschutz auch adressiert findet – Geschäftsmodelle auf der Basis von Kundendaten etwa sind bereits länger und sehr kritisch im Gespräch – das aber in seiner Natur oft weniger angreifbar scheint als die Technik. Es muss aber natürlich auch die Möglichkeit bestehen, in Geschäftsprozesse und -praktiken mit im Gesetzessinne widerrechtlichen Absichten einzugreifen und diese zu verbieten. Diese Möglichkeit besteht und wird auch wahrgenommen, tritt aber in vielen Debatten hinter den technischen Probleme zurück. Beides muss aber gemeinsam betrachtet werden.

Kontrollaufgabe 3.1: Privatheit

Welche Werte und Rechte werden mit Privatheit assoziert? Wie müssen Interpretationen neuer Umstände erfolgen?

K

3.5 Informationelle Selbstbestimmung

Eine besondere Variante der Konzeption des Datenschutzes findet sich in Deutschland. Es ist die informationelle Selbstbestimmung. Zuerst zu ihrer Geschichte. Die informationelle Selbstbestimmung ist begrifflich 1971 in einem Aufsatz von Steinmüller und Lutterbeck enstanden, die das Recht auf informationelle Selbstbestimmung in einem Gutachten für das Innenministerium als allgemeines Persönlichkeitsrecht formulierten. In seiner gegenwärtigen rechtlichen Variante ist die informationelle Selbstbestimmung aber erst 1983 entstanden, und zwar als Reflex auf eine versuchte Volkszählung. Es gab lange und deutliche Proteste gegen diese Volkszählung. Die Menschen fühlten sich unrechtmäßig ausgespäht durch den Staat und hatten den Eindruck, der Staat wolle sie „gläsern“ machen, transparent und damit kontrollierbar. Dieser Eindruck entstand unter dem Einfluss des faschistischen Regimes und des Kontrollregimes der DDR, das sich intensiv der Überwachung bediente, um seine Bevölkerung zu kontrollieren.

Entstand als Reflex auf Volkszählung

Exkurs 3.1: Geschichtlichen Rahmenbedingungen der Volkszählung

E

Einer der Gründungsväter der Idee der informationellen Selbstbestimmung wie ihrer juristischen Implementierung, Werner Steinmüller, schildert die geschichtlichen Rahmenbedingungen der Volkszählung wie folgt:

„Die Volkszählung, um die es hier ging, war historisch, rechtlich wie politisch ein Unikat. Ihre – nicht in der Wahrnehmung einer desinformierten und aufgeheizten Öffentlichkeit – entscheiden – den Punkte waren: Bei der „VZ ’83“ ging es nicht um eine zu weit gehende Ausforschung der Bevölkerung, auch nicht um illegitimes Eindringen in individuelle Intimsphären, sondern um die Ausführung eines lang gehegten Planes der Sicherheitsbehörden („Verfassungen vergehen, Verwaltungen bleiben bestehen“ – so ein berühmter Verwaltungsrechtler der Weimarer Zeit).

Es sollte nämlich nach der 1978 gescheiterten Einführung eines Personenkennzeichens (erster Versuch war 1944 in Gestalt des Personalausweises in den „Protektoraten“; im Reichsgebiet wagte man ihn nicht einzuführen, weil man negative Folgen für die Kriegsmoral befürchtete) ein weiterer auf die NS-Zeit zurückgehender Plan (des Reichssicherheitshauptamtes) ausgeführt werden, mit dem gleichen Ziel der Erfassung der Gesamtbevölkerung (einschl. Ausländer). Nur was 1938 mittels eines Einwohnerinformationssystems realisiert werden sollte, scheiterte damals an den unzureichenden technischen Mitteln.

Nun aber konnte das Vorhaben dank der elektronischen Datenverarbeitung und bestimmter organisatorischer Vorkehrungen (die keines Gesetzes bedurften, weil sie für sich genommen keinen Rechtseingriff enthielten) wesentlich eleganter realisiert werden: durch ein nur wenige Daten umfassendes Zentralregister, das zur Beruhigung der Öffentlichkeit den alten Namen „Melderegister“ beibehalten sollte, aber als eine Art elektronisches Personenkennzeichen konzipiert wurde, das die übrigen Register und Dateien des Staates (ursprünglich: auch der Wirtschaft) erschließen und zusammenführen konnte. – Diesem hehren Ziel diente auf solcherart verschlungenen Wegen das Volkszählungsgesetz.

Damit wäre der Zugriff der Staatsorgane wie der Wirtschaft auf die Daten der Gesamtbevölkerung wie ihrer Teile ermöglicht worden, damals für Kriegs-, heute für unbekannte künftige Zwecke, vor allem der Sozial- und Sicherheitsbehörden. (Wie man inzwischen weiß, hatte bereits die DDR neben Israel beides, Personenkennzeichen und Zentralregister, in aller Stille realisiert, verständlicherweise beschränkt auf den Staat.)“

Aus: Werner Steinmüller, Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann, in: FIfF Kommunikation 3/07

Zu diesem Zeitpunkt war eine Generation Deutscher politisch aktiv, die als Kindergeneration der Nazigeneration eine bis heute verdienstvolle intensive Auseinandersetzung mit diesem Teil der deutschen Vergangenheit begonnen hatte. Überwachung, das war damals klar, war ein Mittel totalitärer Regime und inakzeptabel. So wurde also gegen die Volkszählung demons-

triert und die Proteste waren so intensiv, dass schließlich das berühmte „Volkszählungsurteil“ gesprochen wurde.

Es referiert auf den

D

Definition 3.1: Artikel 8, Absatz 1 der Europäischen Menschenrechtskonvention

„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“

und führt folgend aus, das hier vor allem die individuelle Selbstbestimmung über das eigene Leben als Rechtsgut geschützt werden soll. Dabei gilt dann:

„Individuelle Selbstbestimmung setzt aber - auch unter den Bedingungen moderner Informationsverarbeitungstechnologien - voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung BVerfGE 65, 1 (42) BVerfGE 65, 1 (43) tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen." (BVerfGE 65, 1 – Volkszählung, Zeilen 154, 155)

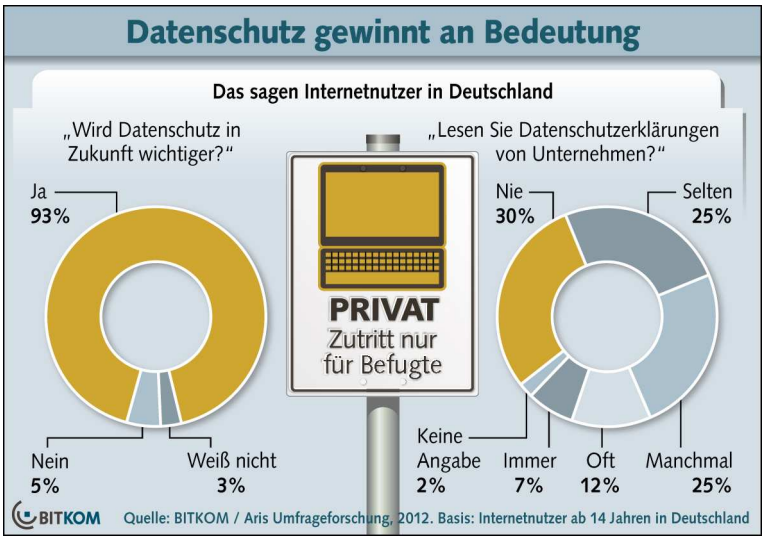


Abb. 3.2: Datenschutz wird in Deutschland als wichtiges Schutzgut wahrgenommen.

Quelle: http://it-news-blog.com/wp-content/uploads/2012/09/Datenschutz.jpg

Damit wurde eine sehr wichtige Einsicht von Lutterbeck und Steinmeier festgehalten, die auch schon von Foucault in dessen Analyse des „Panopticons" von Bentham gemacht wurde: Wer von Autoritäten beobachtet wird, verhält sich möglicherweise anders (in vorauseilendem Gehorsam, aus Angst oder – ex negativo – aus Protest) als ohne Autoritäten und entscheidet so also nicht mehr frei über sein Schicksal. Das ist einmal ein Eingriff in das Menschenrecht auf freie Entfaltung der Persönlichkeit. Dann ist es aber auch eine wichtige Einschränkung einer Demokratie. Denn wenn deren Bürger sich nicht frei entscheiden, können sie auch nicht genuin demokratisch wählen.

Eine informationelle Selbstbestimmung als Kontrolle darüber, wer über welche Informationen über einen verfügt, ist also auch eine Bedingung für die Demokratie.

Das ist nun aber erst einmal nur die Theorie. Praktisch ist die informationelle Selbstbestimmung in der gegenüber den 70ern weiterentwickelten Informationsgesellschaft nur schwierig durchzusetzen. Der Fluss der Daten, damals

noch ein spärliches Rinnsal und recht übersichtlich, hat sich in eine ozeanische Strömung gewandelt und ist in Geschwindigkeit und Masse sowie in Ausdehnung faktisch nicht mehr so einholbar, dass man informationelle Selbstbestimmung in voller Form herstellen könnte. Beim durchschnittlichen Surfen im Internet ist bereits grundlegend unklar, wer was über einen erhebt, wo diese Daten entstehen, wohin sie wandern, was mit ihnen gemacht wird und wie man mit deutscher Datenschutzgesetzgebung dort rechtlich agieren könnte. Jedes Recht setzt auch seine Durchsetzbarkeit als eine Gelingensbedingung voraus, und die ist in diesem Fall nicht mehr konsequent (oder auch nur annähernd) gegeben.

Man darf allerdings mit Recht Zweifel an einem allzu kategorischen Urteil aus dieser Fatalität anmelden, denn in vielen anderen Kontexten, in denen etwa ein Staat Daten erhebt oder eine Firma in einer bestimmten Verwendung, lassen sich die Daten wieder recht gut verorten, technisch wie juristisch, und infolgedessen auch regulieren. An diesen Stellen ist informationelle Selbstbestimmung also durchaus herstellbar und einklagbar.

Kontrollaufgabe 3.2: Informationelle Selbstbestimmung

Was ist die informationelle Selbstbestimmung? Erläutern Sie, ob Sie die informationellen Selbstbestimmung noch aktuell oder für sich selbst als relevant empfinden.

K

3.6 Das Bundesdatenschutzgesetz

Im Folgenden wollen wir uns nun mit dem Bundesdatenschutzgesetz (folgend auch BDSG) beschäftigen, wobei es uns – ganz nach Warren und Brandeis – nicht um eine längliche juristische Besprechung gehen soll. Das werden die Juristen an anderen Stellen besser liefern können. Wir wollen hier die informationsethischen Implikationen, die Absichten und erste Indizien auf die Anwendung im Bereich der Strafverfolgung sowie der nachrichtendienstlichen und militärischen Informationsgewinnung besprechen.

3.6.1 Prinzipien

Das BDSG gehorcht verschiedenen Prinzipien, die als Leitlinien des Datenschutzes in juristischer wie in praktischer Hinsicht zu verstehen sind. Wir werden sie im Folgenden genauer besprechen.

Verbot mit Erlaubnisvorbehalt

Das erste Prinzip adressiert eine wichtige Rangfolge im Umgang mit Daten. Und zwar ist das Erheben von Daten nicht grundsätzlich erlaubt und kann später eingeschränkt oder angeklagt, sondern es ist grundsätzlich verboten und erfordert besondere Genehmigung. Damit ist ein Versuch gemacht, zumindest eine Übersicht zu sichern, wer welche Daten auf welche Weise und in welcher Absicht erhebt und gleichzeitig eine grundlegende Gesetzeskonformität einzuziehen.

Datensparsamkeit und Datenvermeidung

Als nächstes Prinzip gilt, dass jede Erhebung von Daten sparsam erfolgen muss. Insbesondere sollen nur so wenig Daten wie möglich verarbeitet werden, es darf nicht wahllos gesammelt werden, und Daten dürfen nur einen möglichst kleinen Zeitraum gespeichert werden.

Transparenz

Mit diesem Prinzip ist festgehalten, dass jeder Betroffene einer Datensammlung wissen soll, dass Daten über ihn erhoben werden. Bei der Strafverfolgung gelten hier selbstverständlich Ausnahmen, da in diesem Falle die Betroffenen ja gerade nicht wissen sollen, dass sie besammelt werden. Andere heimliche Datensammlungen sind allerdings explizit nicht erlaubt, beziehungsweise nur unter strengen Regeln und Voraussetzungen.

Erforderlichkeit und Verhältnismäßigkeit

Daten dürfen nicht einfach so oder für wenig relevante Zwecke erhoben werden. Sie müssen erforderlich sein. Dabei gilt etwas als erforderlich, wenn es das erträglichste Mittel zur Erreichung der Zwecke der Datenerhebung und –verarbeitung ist. Dabei ist auch die Verhältnismäßigkeit zum Zweck der Datenerhebung zu beachten.

Zweckbindung

Ein weiteres wichtiges Prinzip ist die Zweckbindung der Datenverarbeitung. Daten dürfen nicht zweckfrei erhoben werden oder von einem Zweck in einen anderen migriert werden. Sie müssen für eine bestimmte Absicht erhoben werden und dürfen folgend auch nur in diesem Sinne weiter genutzt und bearbeitet werden.

Richtigkeit und Aktualität

Daten müssen außerdem richtig sein, es dürfen also keine falschen Daten über eine Person angesammelt sein, die dann folgend etwa unverhältnismäßige Konsequenzen für diese Person nach sich ziehen. Daten müssen außerdem auch aktuell sein, um keine verschobenen Urteile nach sich zu ziehen.

Datensicherheit

Schließlich müssen Daten auch sicher gespeichert und bearbeitet werden, so dass kein Dritter an diese Daten herankommt und sie eventuell missbräuchlich verwenden kann.

Neben den genannten Prinzipien gibt es noch weitere wie die Nicht-Diskriminierung, die Haftung oder die Mitsprache, aber diese sind gegenwärtig weniger relevant. Wir wollen nun diesen Prinzipien im Bundesdatenschutsgesetz an einigen kritischen Stellen nachspüren.

Kontrollaufgabe 3.3: Prinzipien des Datenschutz

Welche Prinzipien bestimmen den Datenschutz? Wie hängen diese Prinzipien mit den Persönlichkeitsrechten und mit der informationellen Selbstbestimmung zusammen?

K

3.6.2 Die Prinzipien im Gesetz

In diesem Abschnitt wollen wir nun einige Abschnitte unseres BDSG genauer betrachten, um die festgehaltenen Prinzipien und mögliche Interpretationen zu identifizieren. Zuerst müssen wir dabei die allgemeinen Festlegungen zu Zweck und Anwendungsbereich des Gesetzes ansehen.

Definition 3.2: BDSG, § 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

D

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem

> anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

Hier wird also bereits zu Beginn festgehalten, dass die Datenschutzregelung vor allem dem Schutz der Persönlichkeit dient, wie dies im Volkszählungsurteil bereits angesprochen wurde. Hier liegt folglich auch juristisch der Schwerpunkt des Datenschutzes. Dazu wird festgehalten, dass Datenschutz sowohl für den Staat als auch für nicht-staatliche Institutionen gilt – eine wichtige Regelung, denn ein Großteil der Datenerhebungen erfolgt inzwischen durch private Firmen, die bereits seit Jahren insbesondere in Deutschland besonders streng reguliert werden. Das hohe Gewicht auf Datenschutz in Deutschland hat dabei nur kurzfristig negative Auswirkungen gehabt durch höhere Initialkosten. Folgend wurde von vielen Kunden die hohe Sicherheit der Daten vor dem Zugriff anderer als Vorteil begriffen, so dass der komplizierte und hohe Datenschutz inzwischen ein wichtiges Marktkriterium geworden ist.

Ebenfalls hervorzuheben ist in diesem Kontext die Gültigkeit für jede Variante ausländischer Firmen oder staatlicher Stellen, sofern die entsprechenden Daten im Inland, also in Deutschland erhoben werden.

Die Einschränkung auf das Inland ist notwendig, da das BDSG ein nationales Gesetz ist. Es gibt allerdings auch im internationalen Raum Datenschutzgesetze. Ein besonders wichtiges Gesetz ist die europäische Regelung zu Datenschutz für die EU-Staaten, ein Gegenstand, mit dem wir uns noch später befassen werden.

Schließlich ist auch hervorzuheben, dass das Gesetz den Datenschutz zwischen verschiedenen anderen Werten ansiedelt. Es gilt also nicht absolut, als Gesetz über allem anderen, sondern eingeschränkt. Der Datenschutz ist wichtiger als Verwaltungserfordernisse – das besagt Absatz (4). Er ist aber nicht so wichtig, dass nicht auch Einschränkungen des Datenschutzes möglich sind – Absatz (3). Insbesondere, wenn größere Gefahren drohen, sind Außer-Kraft-Setzungen des Datenschutzes also durchaus möglich. Diese Re-

lativierung entspricht unserem Wertempfinden in diesem Bereich. Anders gesagt: Kriminelle Daten haben kein Anrecht auf Datenschutz. Allerdings besteht die Schwierigkeit der Strafverfolgung nun gerade darin, dass kriminelle Daten (oder anderweitig gefährliche) eben nicht als solche sichtbar sind. Daher greifen in diesem Bereich eine Reihe von Detailregelungen, wann und wie bei möglichen Gefährdungen oder zur Aufklärung krimineller Taten (und damit zur Vermeidung späterer, weiterer Gefährdungen) der Datenschutz aufgehoben werden kann.

Interessant sind nun weiter auch die Begriffsbestimmungen, die im BDSG zu den verwendeten Begriffen gesetzt werden.

D

Definition 3.3: BDSG, § 3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,

2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

3. Übermitteln das Bekanntgeben gespeicherter oder durch

Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass

a) die Daten an den Dritten weitergegeben werden oder

b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,

5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens

über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

[...]

An diesem Abschnitt sind verschiedene Festlegungen besonders beachtenswert.

Zuerst ist zu beachten, dass die Automatisierung der Datenbearbeitung durch Datenverarbeitungsanlagen bereits angesprochen ist – und zwar, mit dem Begriff „Datenverarbeitungsanlage“, in einer angenehm weiten, zukünftigen Entwicklungen gegenüber aufgeschlossenen Begriffswendung. Dies ist als Bezugspunkt überaus relevant, denn jede Form von Computer oder digitaler Sensor kann hier bereits zum rechtlichen Gegenstand werden. Damit sind Interpretationsspielräume wie in dem oben skizzierten Beispiel des Gerichtsverfahrens von Louis Brandeis ausgeräumt. Strafverfolger oder auch kommerzielle Datensammler dürfen sich nicht auf besondere technische Neuheiten zurückziehen, sondern müssen bei jeder Form der Innovation, sofern sie Kapazitäten der Datenverarbeitung besitzt, das Datenschutzgesetz von Beginn an einbeziehen.

Diese Breite entspricht der Idee, dass Datenschutz als primär wichtig vor Datenerhebung geachtet wird, was sich etwa auch im Prinzip der Datensparsamkeit niederschlägt. Dazu muss auch die Bemerkung „ungeachtet der Verfahren“ im obigen Abschnitt gezählt werden. Hier wird der Umstand einbezogen, dass nicht jede Datenverarbeitung auf technischem Wege stattfinden muss, dass also auch nicht-technische Verfahren einzubeziehen sind, und dass ferner kein Rückzug auf besondere Technologieformen stattfinden darf.

D

Definition 3.4: BDSG, § 3a Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und

keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Dies ist nun eine direkte Entsprechung des Verbots mit Erlaubnisvorbehalt und eben des Prinzips der Datensparsamkeit. Ein besonderes Gewicht kommt zudem der Anonymisierung/Pseudonymisierung zu, die beide als Prozesse aufgeführt werden. Der Nutzen dieser Prozesse ist klar, da hiermit eine weniger starke Personalisierbarkeit der Daten gegeben ist, also automatisch auch eine für das Persönlichkeitsrecht weniger indikative Datensammlung und -bearbeitung. Es dürfen und müssen allerdings gelegentlich Zweifel an Verfahren der Anonymsierung/Pseudonymisierung angemeldet werden, da diese Prozesse nicht notwendig immer das notwendige Maß an Schutz der Persönlichkeit entfalten. Auch wenn Namen entfernt sind, lassen sich über Querverbindungen wie etwa Wohnort, Arbeitsplatz und Position, Tätigkeiten noch Rückschlüsse auf die Personen hinter den „anonymen“ Daten machen. Diese impliziten Schlüsse sind insbesondere aufgrund neuer Verfahren in der Forensik und der Auswertung von Daten („Big Data“) zu Spionagezwecken immer besser möglich und immer präziser. Das Maß der Anonymisierung müsste diesen Fortschritten also angepasst werden, was aber nicht immer einfach ist.

D

Definition 3.5: BDSG, § 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder

b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,

2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und

3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

Hier nun finden sich der Vorrang des Verbots und der Geist der informationellen Selbstbestimmung gut wieder. Es wird keine pauschale Zulässigkeit ausgegeben, sondern im Gegenteil eine enge Zweckbestimmung vorgeschrieben. Außerdem soll ein jeder potentieller Betroffener jederzeit Einsicht in seine Daten haben können. Mit dieser Festlegung und der Bestimmung der dafür notwendigen Rahmenbedingungen wird die Möglichkeit der informationellen Selbstbestimmung angelegt.

Eine weitere Verstärkung des Vorrang des Verbots findet sich in folgendem Paragraph, der als Ergänzung beachtet werden muss.

D

Definition 3.6: BDSG, § 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nichtöffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Dabei wird in diesem Paragraphen auch die persönliche Haftbarkeit sichergestellt, eine wichtige Ergänzung, ohne die Verantwortung schnell abgewiesen werden könnte. Viele weitere Abschnitte des BDSG sind ebenfalls im Kontext der bereits diskutierten Prinzipien und der zugrundeliegenden Diskussionen über Privatheit als Persönlichkeits-, als Menschenrecht und in Gestalt informationeller Selbstbestimmung zu betrachten. Für eine vertiefte Betrachtung sei hier auf die juristischen Arbeiten zu diesem Thema hingewiesen. An dieser Stelle geht es eher um das prinzipielle Verständnis. Dieses grundlegende und prinzipielle Verständnis ist in gewisser Weise ohnehin in vielen Situationen wichtiger als konkrete Vorschriften, da sie ein allgemeineres Verständnis des Erlaubten und des Verbotenen erlauben. Damit kann man flexibler und direkter Situationen beurteilen, die sich aufgrund ihrer Umstände konkreten Vorschriften entziehen.

3.7 Probleme bei der Anwendung des Datenschutzes

Leider ist der Datenschutz nicht immer einfach anzuwenden. Dies ist ein Problem, das auch informationsethisch relevant ist, denn eine mangelhafte Umsetzung von Recht muss als eigenes Werteproblem anerkannt und in mögliche Erwägungen von Wertgewichtungen aufgenommen werden. Würde sich zum Beispiel herausstellen, dass Datenschutz in einem bestimmten Produkt überhaupt nicht herstellbar ist, so müssten Überlegungen angestrengt werden, ob dieses Produkt an sich tragbar sein kann oder ob es nicht abgeschafft werden müsste. Sehen wir uns einige Probleme im Detail an.

3.7.1 Interpretative Freiräume

Ein in verschiedenen Kontexten immer wieder auftretendes Problem sind mögliche alternative Interpretationen von Rechtstexten, von Vorschriften oder anderen Richtlinien im Datenschutz. Dies gilt insbesondere dann,

wenn sich die kontextuellen Bedingungen des Problems signifikant verändern. Das BDSG ist aus diesem Grund besonders weit formuliert. Wir haben oben die entsprechenden Begriffe und Bestimmungen angesehen. Es sind extra keine spezifischen, sondern unspezifische Kontexte in recht allgemeinen Begriffen angegeben. In unsicheren Situationen sollte man sich folglich eher vorsichtig verhalten und eine maximal datenschutzsensible Interpretation anstreben.

3.7.2 Entwicklungsdynamiken

Eine der größten Herausforderungen für den Datenschutz ist folgend die hohe Dynamik der technischen Entwicklungen und deren Nutzungsformen. Denn insbesondere die Sonderregelungen, die das Datenschutzrecht bei besonderen anderen Gefährdungen aufheben, müssen doch um einiges spezifischer sein, da an diesen Stellen und mit diesen Formulierungen Missbrauch der Sicherheitsbefugnisse zu Ungunsten der Freiheit stattfinden könnten, wenn hier die Formulierungen ebenfalls nur breit und mit hohen Interpretationsspielräumen versehen wären. So äußert sich im Grad der Präzision von Vorschriften erneut die Vorliebe für Freiheit vor Sicherheit und für den Vorrang des Verbots. Muss man allerdings hier sehr spezifisch für besondere Technologieformen formulieren, hinkt man häufig hinter den technischen Entwicklungen hinterher. Der Markt der Consumer Electronics ist in der Regel doch bedeutend schneller als der Gesetzgeber. Damit ergeben sich immer wieder neue „Schlupflöcher“ für die Ermittler, Vorschriften zugunsten der Sicherheit auszulegen. Bekannt ist hier etwa die Quellen-TKÜ-Vorschrift (Quellen-Telekommunikationsüberwachung), die lange Jahre vor der digitalen Revolution genau regelte, welche technischen Kommunikationen in welcher Granularität abgehört werden konnten. Da nun allerdings die Abhörung von Telefonen eine grundlegend andere Sache war als die von Datenverbindungen, war es lange Zeit möglich, wesentlich mehr Daten abzugreifen, als es im Sinne des Gesetzgebers war. Denn das Anklemmen an eine Telefonleitung hat nur einige wenige Telefongespräche freigegeben. Das Anklemmen an eine Datenverbindung dagegen gibt wesentlich mehr von den Betroffenen bekannt. Hier ist also ein Beispiel dafür, wie neue Technologien Probleme für Interpretationen schaffen können.

3.7.3 Komplexität

Ein weiteres, ebenfalls schon länger hinlänglich bekanntes und nur schwer lösbares Problem ist die enorm hohe technische und regulative Komplexität der Informationstechnologien. Die technische Komplexität findet sich auf

vielen verschiedenen Ebenen wieder. Sie betrifft einerseits die Netzwerke, ihre Protokolle und ihre Organisation, die Datenwege allgemein. Diese sind zum Teil schwierig zu kontrollieren, kaum einzusehen, so dass Transparenz nur schlecht herstellbar ist. Ohne Transparenz aber kann auch nicht gewährleistet werden, dass eine jeder potentiell Betroffener noch informationelle Selbstbestimmung herstellen kann. Sobald seine Daten in Netzwerke wandern, wird er Schwierigkeiten haben, noch mit hoher Sicherheit festzustellen, wo sie sonst noch hinwandern. Das Gleiche gilt für verschiedene Anwendungen oder Dienste, die von Nutzern verwendet werden. Auch hier ist oft undurchsichtig, was mit einmal erhobenen Daten passiert. Die technischen Optionen der Speicherung und der Verteilung, des Kopierens und des Nutzens sind schlicht zu zahlreich, um alle Varianten sicher auszuschließen. Hinzu kommt, dass die rechtlichen Bedingungen des Datenschutzes und insbesondere spezifische auftretende Bedingungen bei Vertragsabschlüssen mit Softwareunternehmen und Dienstleistern, die den Datenschutz einschränken können, ebenfalls ungewöhnlich komplex sind. In diesem Fall handelt es sich zwar um die begriffliche Komplexität juristischer Fachformulierung, die also prinzipiell zugänglich ist. Auf den Laien jedoch wirken diesen begrifflichen Komplexitäten nicht weniger tatsachenverschleiernd als die technischen und sorgen also auf andere Weise für Unsicherheit und ein Unvermögen zur Transparenz. Ein hier viel zitiertes Beispiel sind License Agreements, also jene Texte, die bei neuen Nutzungen von Anwendungen und Diensten regelmäßig aufkommen und bei denen per Click bestätigen muss, dass man sie zur Kenntnis genommen und akzeptiert hat. Hier ist bekannt, dass diese Texte so gut wie niemals gelesen werden – und dass sie genau deshalb oft genutzt werden, um „Einwilligungen“ zu massiven Datenabflüssen einzuholen.

3.7.4 Globalität

Dabei kommt schließlich noch hinzu, dass viele der diese Anwendungen und Dienste anbietenden Unternehmen im Ausland sitzen und sich nur begrenzt um das deutsche Datenschutzrecht sorgen müssen. Für größere Unternehmen gilt zumindest auf deutschem Boden natürlich das Gesetz mit aller Strenge, und es müssen entsprechende Vorkehrungen gemacht und bewiesen werden. Aber selbst diese großen Unternehmen leiten Daten oft über ihre Zentralen im Ausland, und viele kleinere Firmen bearbeiten Daten prinzipiell im Ausland, so dass für diesen Fall also kein deutsches und in vielen Fällen einfach gar kein Datenschutzrecht gilt. Die Daten können erhoben, gespeichert und bearbeitet werden, wie es den entsprechenden

Unternehmen gerade gefällt. Dies schließt auch die Option ein, dass die Sicherheitsdienste dieser anderen Länder die Daten über Deutsche verwerten dürfen, um sicherheitsrelevante Informationen zu gewinnen. PRISM war hier ein indikativer Vorfall.

K

Kontrollaufgabe 3.4: Durchsetzung des Datenschutzes

Welche Probleme treten bei der Durchsetzung des Datenschutzes auf? Wie prägen sich diese auf die zugrundeliegenden Werte der Informationsethik aus?

3.8 Datenschutz – quo vadis?

Die Probleme sind nur die Spitze eines ganzen Eisbergs möglicher Probleme mit dem Datenschutz. Infolgedessen ist es auch wenig überraschend, dass immer wieder gravierende Vorfälle mit Daten bekannt werden und dass folgend das Vertrauen in den Datenschutz nicht besonders hoch ist oder weiter sinkt. Vertrauen ist eben eine sehr flüchtige Einstellung, die nicht leichtfertig verspielt werden darf und die sehr schwer wiederzugewinnen ist.

Der Verlust des Vertrauens kann sich dann direkt und drastisch auf die informationelle Selbstbestimmung ausprägen, denn diese muss dann einem Eindruck einer informationellen Fremdbestimmung weichen, der die politische Handlungsfähigkeit der Demokratien unerträglich einschränken kann. Besonders schlimm aber trifft die moderne Überwachungsmaschinerie IT und Internet die Bürger totalitärer Staaten. Für diese Staaten ist das Internet ein wahres Gottesgeschenk der Kontrolle. Dies ist eine besonders fatale Entwicklung, der im Rahmen der Datenschutzdiskurse nicht genug Aufmerksamkeit geschenkt wird.

3.9 Zusammenfassung

Dieser Studienbrief gab Ihnen einen Überblick über den Datenschutz und dessen Bedeutung. So wurde zunächst im Abschnitt 3.3 Einführung – Öffentlich und Privat als Kennzeichnung von Information grundlegend die Kennzeichnung von Informationen diskutiert und ihre Relevanz für die Öffentlichkeit dargelegt. Des Weiteren wurde die Abgrenzungen von Informationen, die für die Öffentlichkeit bestimmt sein sollen und welchen, die es nicht sind, beleuchtet und festgestellt, dass die Übergänge fließend und im stetigen Wandel sind.

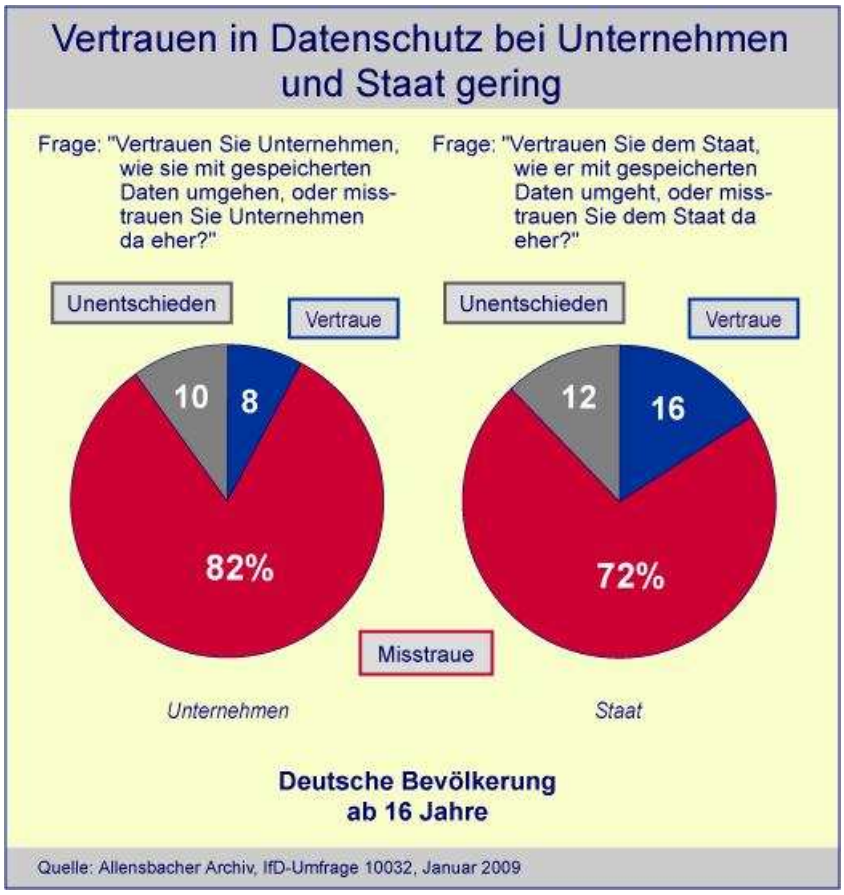


Abb. 3.3: Das Vertrauen in den Datenschutz ist oft nicht gut.

Quelle: http://www.itespresso.de/files/2008/images/20090508_datenschutz-umfrage/2009_allensbach-umfrage_datenschutz_1.jpg

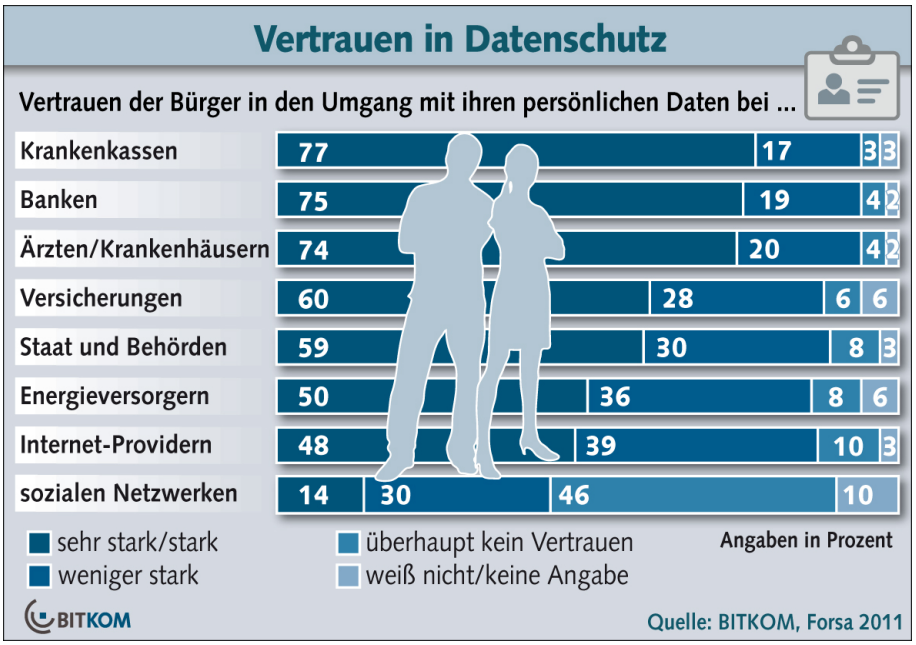


Abb. 3.4: Das Vertrauen in Datenschutz variiert nach Datenhalter.

Quelle: http://www.bitkom.org/files/documents/Datenschutz_Download.jpg

In dem Abschnitt 3.4 The Right To Be Left Alone wurde die Privatheit in den USA näher betrachtet, die im 4th Amendement geregelt ist. So wurde auch die zeitgemäße Interpretation des Datenschutzes angesprochen, die Privatheit durch technologischen Fortschritt weiter gewähren soll.

In dem darauffolgenden Abschnitt 3.5 Informationelle Selbstbestimmung wurde die Intension und ihr Ursprung näher erläutert. So wurde dargelegt, dass jeder entscheiden darf, wer was über einen wissen sollte. In dem Abschnitt 3.6 wurde das Bundesdatenschutzgesetz besprochen. Dabei wurde auf die allgemeinen Prinzipien und wie diese im Gesetz sich widerspiegeln dargestellt.

In den letzten beiden Abschnitten 3.7 Probleme bei der Anwendung des Datenschutzes und 3.8 Datenschutz – quo vadis? werden die datenschutzrechtlichen Probleme durch neue Technologien und Überblick auf die aktuelle Entwicklung des Datenschutz gegeben.

3.10 Übungen

Ü

Übung 3.1: Kommerzielles Data Mining

Ein kommerziell orientiertes App-Unternehmen will Daten seiner Nutzer erheben und diese verwerten. Erläutern Sie auf einer allgemeinen, vorjuristischen Ebene, welche Prinzipien des Datenschutzes davon betroffen sind und wie sich das Unternehmen verhalten muss und kann, um datenschutzkonform zu agieren.

Ü

Übung 3.2: Datenschutz und Sicherheitsbedarfe

Für ein Ermittlungsverfahren müssen digitale Kommunikationen möglicher Verdächtiger beobachtet werden. Erläutern Sie aus dem vorangegangenen Brief zur Sicherheitsrationalität, welche Prinzipien der Sicherheit hier greifen und diskutieren Sie folgend die möglichen Interaktionen dieser Prinzipien und Werte mit denen des Datenschutzes und der Privatheit.

Ü

Übung 3.3: Datenschutz und Sicherheit

Wie sieht für Sie der Konflikt zwischen Privatheit und Sicherheit aus? Erläutern Sie Ihre Wahrnehmung des Konflikts und formulieren Sie Ihr eigenes Wunschmaß für die Balance zwischen Sicherheit und Freiheit in digitalen Räumen. Verargumentieren Sie dabei alle in den vergangenen beiden Texten vorgekommenen Punkte.

Studienbrief 4 Wert und Strukturen der Sicherheit und Freiheit in Cybercrime

4.1 Lernziele

Was wird Ihnen vermittelt?

Der folgende Abschnitt wird eine Einführung in das Problem der Anwendung von Informationsethik auf das Feld Cybercrime liefern. Dabei wird auf die besonderen Probleme bei Strafverfolgung eingegangen und Lösungsansätze darstellen.

4.2 Advanced Organizer

Der Studienbrief 4 Wert und Strukturen der Sicherheit und Freiheit in Cybercrime setzt die Kenntnisse aus den vorherigen Studienbriefen voraus.

4.3 Informationsethik und Cybercrime

Wo liegt hier eigentlich das Problem?

Der Kriminalist muss eine Reihe von Tätigkeiten im Cyberspace ausführen können, um Straftaten erkennen und verfolgen zu können. Er muss kriminelle Handlungen als solche erkennen können, sich Zugang zu tatsächlichen und potentiellen Tatorten verschaffen können, zu Zeugen und Opfern, zu Spuren und Wegen, und er muss Spuren auf Täter abbilden können. All diese Teilschritte bedingen nun allerdings Handlungen des Kriminalisten im digitalen Substrat, die mit dessen Natur interagieren müssen und die teilweise ihre eigenen Voraussetzungen überhaupt erst herstellen müssen.

Physikalische Spuren

Ein prominentes Beispiel sind digitale Spuren. Digitale Spuren sind von grundsätzlich anderer Natur als physische Spuren. Physische Spuren lassen sich zwar ebenfalls vertuschen und sabotieren, aber nur durch physische Handlungen an diesen Spuren, die also streng genommen nur eine Veränderung dieser Spuren vornehmen und keine „Auslöschung“. Außerdem sind physikalische Spuren – wie uns viele moderne Crime-Fernsehserien schon lehren – sehr zahlreich und die Polizei ist in der Regel weit besser

Digitale Spuren

in der Lage, diese Spuren zu erkennen und zu sichern als der Täter. Bei digitalen Spuren dagegen ist das völlig anders. Sie stellen keine eindeutigen Kausalketten mit möglichen Bemühungen ihrer Beseitigung her. Wenn ein Datum auf einem digitalen Speicher etwa überschrieben wird, dann ist dieses Datum absolut unwiderruflich und ohne „Restspuren“ verloren. Auch eine Rückverfolgung des Prozesses, der die Spur gelöscht hat, bringt meist nur sehr wenig. Da sich sowohl Daten wie Prozesse auf den gleichen Speicherabschnitten austoben, überschreiben sich alle möglichen Prozesse und Daten immer wieder gegenseitig, so dass also auch ein völlig legitimer Prozess Datenspuren löschen kann und so dass auch ein Prozess eines Angreifers selbst schnell wieder gelöscht ist, wenn er sich nicht irgendwo dauerhafter eingerichtet hat. Ohne Spuren allerdings kann der Strafverfolger seiner Verantwortung nicht nachkommen und den Wert der Sicherheit nicht realisieren. Er lässt zu, dass andere verletzt und geschädigt werden. Für den Strafverfolger besteht also ein Interesse, die Spuren zu „persistieren“. Sie müssen dauerhaft gemacht werden, um in einem Straffall in einer Menge existierenden Indizien arbeiten zu können. Nun ist allerdings das nächste Problem, dass man in der Regel vor einer digitalen Straftat

nicht weiß, welche Daten an welchen Orten denn im Einzelnen besonders relevant sind. Dies weiß man erst danach, oft sogar erst sehr viel später danach. Also, so der Rückschluss, müssen einfach alle Daten für eine Weile persistiert werden, um dann bei Meldung eines Verbrechens innerhalb eines gewissen Zeitraums noch darauf arbeiten zu können. So weit, so gut. Nun allerdings tritt der bereits beschriebene panoptische Effekt auf den Plan. Wenn wirklich absolut alle potentiellen Spuren im Internet dauerhaft gemacht werden, entspricht dies einer lückenlosen Überwachung des Netzes. Dies kann dann wiederum die Freiheit vollkommen unbescholtener Bürger sehr nachhaltig beeinträchtigen und vor allem sehr umfassend, da das Internet ja inzwischen wirklich überall ist. So kommt also ein Wertekonflikt zustande. Sicherheit – so scheint es zumindest in dieser noch begrenzten Betrachtung – lässt sich nur auf Kosten der Freiheit realisieren und umgekehrt.

Dieses Problem – wir erkennen es als den Kernkonflikt zwischen Sicherheit und Freiheit – findet sich nun im Umfeld des Cybercrime und seiner Bekämpfung an verschiedenen Stellen wieder, die wir uns in diesem Studienbrief genauer ansehen wollen.

4.4 Werte und Strukturen

Zunächst aber wollen wir etwas genauer auf Möglichkeiten der qualifizierten Besprechung eines ethischen Konflikts eingehen. Was tut man in einem Wertekonflikt? In der realen, weniger philosophischen Welt wird das Thema politisiert. Pole bilden sich, und es wird gestritten, wobei sachliche Argumente oft in den Hintergrund treten, weil sie sich schlecht anbringen lassen oder weil Emotionen den Sachargumenten andere Intensitäten verleihen. Was dem Einen harmlos und vernachlässigbar vorkommt, ist dem Anderen unglaublich wichtig und zentral. Ein diskursiver Prozess beginnt damit, in dem sich die Konfliktparteien vielfach wandeln, ausdehnen, aufsplittern, Positionen verändern, bis schließlich Kompromissmöglichkeiten gefunden und ausgehandelt werden können. Dieser Prozess ist wissenschaftlich hochinteressant – allerdings für die Informationsethik nur aus einer Metaebene. Denn die Informationsethik ist eine normative Disziplin. Sie interessiert nicht, wie etwas tatsächlich abläuft, sondern wie nach etwas ethischen Gesichtspunkten abzulaufen hat.

Entscheidungen in Wertkonflikten sind allerdings auch aus normativer Ebene alles andere als einfach. Es gibt verschiedene Verfahren dafür. Einfach

liegt der Fall, wenn Werte in einer entweder kausal oder kulturell eindeutig verankerten Hierarchie zueinander liegen.

Gibt es dagegen aufgrund der besonderen Bedingungen eines Konflikts keine klare Hierarchie, liegt der Fall anders. Eine Methode lässt sich von dem berühmten Philosophen John Rawls ableiten. Rawls war ebenso wie viele andere Philosophen von dem Umstand fasziniert, dass es viele unterschiedliche politische Systeme mit ganz verschiedenen Vorstellungen von Gerechtigkeit gibt. Für streng logisch und rational orientierte Philosophen, die zudem das Problem der Entscheidung von Werthierarchien zu lösen habt, ist das eine seltsame und unangenehme Tatsache. Gerechtigkeit scheint eine recht klare und eindeutige Idee zu sein, aber dennoch gibt es starke Unterschiede in ihrer Anwendung – mit je hoher Akzeptanz unter den Betroffenen. Wie lässt sich so etwas also in einem Verfahren festmachen? Rawls Antwort war der Schleier des Unwissens. Man sollte sich seine Gesellschaft vorstellen und dabei alle Werthierarchien vorzeichnen, wobei man aber einbeziehen sollte, dass man nicht wissen könne, in welcher Rolle man später in dieser Gesellschaft vorkommt – ob ganz Oben oder ganz Unten, männlich, weiblich, mit Arbeit oder ohne. Dieses Unwissen soll dann bei den Entscheidenden eine gerechte Entscheidung produzieren.

Den Fall von beiden Seiten betrachten

Übertragen auf unser Eingangsbeispiel bedeutet dies, dass man sich sowohl in die Situation eines Opfers von Cybercrime als auch in die eines Opfers von Überwachung versetzen muss, um entscheiden zu können, mit welcher Variante man gesellschaftlich leben kann und welche Variante weniger erträglich ist. Allerdings muss man in diesem Verfahren in der Lage sein, die resultierenden Situationen gut abzuschätzen, und man sollte nicht nur nach seinem subjektiven Empfinden, sondern auch nach rationalen Koordinaten wie dann entstehenden Konflikten mit Werten emotional Ausschau halten. Die Grundfrage aber bleibt: Will ich in so einer Welt leben, wenn ich auch auf der „anderen“ Seite stehen könnte?

Komplexer Abwägungsprozess

Prozess und Ergebnis bei Rawls Verfahren sind leider nicht einfach und oft auch nicht eindeutig. Bei der Absehung aller Konsequenzen gibt es stets hohe Unsicherheiten. In unserem Beispielfall etwa wird immer wieder vorgebracht, dass wir nicht einer Diktatur leben, sondern in einem funktionierenden Rechtsstaat, so dass also Überwachung einen ganz anderen Charakter hat. Die Frage ist allerdings, wie stabil denn dieser Rechtsstaat ist und wie sicher wir sein können, dass innerhalb der Lebensdauer dieser technischen Paradigmen – und ein Ende ist nicht absehbar – nicht doch

ein Rückfall in eine stärker totalitäre Regierung möglich ist. Da wir zumindest keine harten Kriterien haben und haben können, wie sich so etwas verhindern lässt, sollten wir diese Möglichkeit mit einbinden. Überzeugte Demokraten sehen das aber anders und behandeln diese Möglichkeit oft als abwegig. Was wäre hier also die richtige Vorstellung, in die man sich versetzen sollte? Und auch auf der Seite der Opfer von Cybercrime ist ein breites Spektrum der Möglichkeiten vorhanden, an dessen extremem Ende der Ruin des Landes durch strategische kompetitive Industriespionage steht – mit den entsprechenden Folgen für Wohlstand, Freiheit und Sicherheit. Sollte man von diesem Fall ausgehen oder von einem anderen? Und von welchem? Wir werden gleich noch auf die Frage nach dem Umgang mit Komplexität eingehen. Aber selbst mit einfachen Positionen in der Szenarioentwicklung muss man nicht unbedingt zu einer Lösung kommen. In unserem Beispiel ist es gut möglich, dass man weder ein Opfer von Cybercrime, noch ein Objekt der Überwachung werden will. Was dann?

Rawls Verfahren muss also wiederholt und wiederholt werden, während man das Problem in seine Einzelteile zerkleinert, um zu besseren und klareren Empfindungen zu kommen. Es muss also als Teil des ethischen Prozesses eine umfangreichere Evaluation in verschiedene Richtungen stattfinden, die alle relevanten Komponenten des Konflikts auslotet. Dabei müssen die Handelnden als Akteure und Betroffene in die Überlegungen eingebunden werden, und es muss folgendes herausgefunden werden:

(1) Wertespektrum: Welche Werte sind insgesamt bei allen Handelnden und Betroffenen relevant?

(2) Intensität: Wie intensiv sind diese Werte betroffen? Wie lassen sich unterschiedliche Empfindungen von Intensitäten bei Handelnden dekonstruieren und verstehen? Wie sind diese Intensitäten werthaft begründet oder begründbar?

(3) Relative Intensität: Wie stark ist der Kontrast zwischen den Intensitäten?

(4) Strukturen: Welche Bedingungen liegen für das Handeln der Handelnden vor? Welche davon sind notwendig, welche möglicherweise nur unter bestimmten Bedingungen notwendig, welche sind variabel? Wie rahmen sie das Handeln ein?

(5) Unmittelbare Konsequenzen: Was werden die unmittelbaren Folgen

bestimmter Wertentscheidungen sein? Wie werden die Akteure reagieren und welche Folgeprobleme können direkt entstehen?

(6) Höherstufige Konsequenzen: Was werden die mittelfristigen und langfristigen Folgen bestimmter Wertentscheidungen sein? Wie sind in diesen Entwicklungen andere Werte wieder betroffen? Wie viel Unsicherheit ist bei diesen Abschätzungen einzubeziehen?

(7) Alternative Szenarien: Welche Handlungsalternativen gibt es insgesamt? Wie verändern sich Konsequenzengeflechte unter Anwendungen dieser Alternativen an verschiedenen Punkten?

Dabei kann man erkennen, dass das Zusammenspiel der ersten Fragen (1) bis (3) nach den Werten und der Fragen aus Frage (4) nach den Strukturen die Vorbedingungen für die präzise Evaluierung der weiteren Fragen (5) bis (7) darstellen. Die Werte geben intrinsische Gründe und Ziele des Handelns an, die Strukturen dagegen setzen die weltlichen Bedingungen für das Realisieren dieser Gründe und Ziele. Das Zusammenspiel von Werten und Strukturen ergibt so die möglichen Szenarien und Alternativen, die folgend ethisch evaluiert werden können. Mit ihnen lässt sich eine Karte mit verschiedenen Pfaden anlegen, von denen aus man größere Klarheit über die Lage des Problems erhält sowie über seine verbliebenen „Blind Spots“. Das Verfahren muss allerdings iterativ immer wieder angewendet werden, wenn sich das Problem an sich verändert hat oder wenn sich die Werteverhältnisse verschoben haben.

4.5 Komplexität in der Informationsethik

Ein konstantes Problem in der Technikethik ist die hohe Komplexität der Möglichkeiten, besonders bei komplexen Technologien in komplexen Anwendungsbereichen und bei längerfristigen Perspektiven. Bei hoher Unsicherheit gibt es einige typische Wege, wie sich Akteure unter Einbeziehung von Werten entscheiden:

(1) Wahrscheinlichkeitstendenzen: Man tendiert zu jener Menge von Handlungen, die aufgrund der verschiedenen Wahrscheinlichkeiten am ehesten eine kontrollierbare und positive Entwicklung der Szenarien hervorbringt. Man will hier trotz Unsicherheit vor allem etwas Werthaftes realisieren („man muss doch etwas tun“).

(2) Verantwortungsprinzipien: Man entscheidet nach zuvor besonders

priorisierten Werten oder Prinzipien, welche Variante von Handlungsmengen aus dieser Perspektive besonders ratsam und effizient erscheint – unabhängig von Wahrscheinlichkeiten und anderen Werten. Man will hier trotz Unsicherheit vor allem gemäß seines eigenen Wertekanons handeln („man sollte nach bestem Gewissen handeln“).

(3) Worst-Case Vermeidung: Man orientiert sich an dem aus der eigenen Menge und Hierarchie der Werte heraus schlimmsten Fall, da dieser die höchsten Risiken bietet, und verfolgt die in dieser Hinsicht besonders zielführende Handlungsmenge. Man will hier trotz Unsicherheit das scheinbar Schlimmste vermeiden („das darf auf keinen Fall passieren“).

(4) Best-Case Realisierung: Man orientiert sich an dem aus der eigenen Menge und Hierarchie der Werte heraus besten Fall, da dieser die besten Möglichkeiten bietet, und verfolgt die in dieser Hinsicht besonders zielführende Handlungsmenge. Man will hier trotz Unsicherheit das scheinbar Beste erreichen („das sollte man unbedingt versuchen“).

(5) Entscheidungsenthaltung: Man darf sich auch entscheiden, sich nicht zu entscheiden, bis sich die Situation weiter geklärt hat. Dies stellt allerdings ebenfalls eine Handlung dar, sofern man alternativ handeln könnte, deren Konsequenzen verantwortungsrelevant und damit einzubeziehen sind. Man will hier nicht unter Unsicherheit falsch handeln und die Situation verschlimmern („besser nichts falsch machen“).

Keines der Verfahren ist ethisch besonders ausgezeichnet. Hierfür bräuchte es „Überwerte“, die eine Hierarchisierung der hier sichtbaren leitenden Werte der Entscheidungen selbst korrelieren. Dies lässt sich allerdings nicht klar und widerspruchsfrei angeben.

Sind Probleme besonders komplex und dringt man im Rahmen seiner iterativen Verfahren tiefer in diese vor, so kann man oft kombinierte Varianten dieser Entscheidungen konstellieren. Man kann etwa eine Vorauswahl besonders erfolgversprechender Handlungsstränge treffen, unter denen man folgend nach Prinzipien priorisiert, wobei man Worst Cases und Best Cases besonders berücksichtigt. Dies ist ein gängiges strategisches Entscheidungsmuster, das auch für ethische Entscheidungen anwendbar ist, wobei die ethischen Konflikte und Werte die Konstellationspunkte darstellen.

Im Rahmen dieses Verfahren muss man allerdings aufpassen, dass man es nicht versehentlich manipuliert. In vielen Fällen greifen hier Wahrnehmungsschwierigkeiten, die zuerst von Tversky und Kahnemann geschildert wurden. Die beiden Wirtschaftswissenschaftler haben festgestellt, dass Menschen in Situationen mit unsicherem Wissen automatisch tendenziös werden und auf heuristische Maßnahmen zurückgreifen. Eine „reduzierte Rationalität“ tritt auf. Sie äußert sich in vier Effekten:

(1) Ankereffekt: Zahlen oder Fakten, die vor einer Entscheidung gehört wurden, beeinflussen das Wissen, das für diese Entscheidung herangezogen wird. Tversky und Kahneman haben Probanden gefragt, wie viel Prozent der UN-Nationen afrikanische Staaten sind. Zuvor hatten sie mit den Probanden allerdings ein manipuliertes „Glücksrad“ gespielt, das bei der einen Gruppe meist bei 10 stehenblieb, bei der anderen besonders häufig bei 65. Die Gruppen haben folgend die Prozentzahl der afrikanischen Staaten respektiv kleiner oder höher eingeschätzt. Die erste Gruppe hat im Schnitt 25 % angegeben, die zweite 45 %.

(2) Verfügbarkeitsheuristik: Analog werden auch Urteile von im Gedächtnis besonders präsenten Fakten überlagert. Ereignisse, an die man sich leicht erinnert, scheinen wahrscheinlicher und häufiger als Ereignisse, an die man sich nur schwer erinnert. Auch nicht selbst erlebte, sondern vermittelte Erfahrungen können so wirken. So können insbesondere medial besonders häufig und deutlich vermittelte negative Ereignisse das Urteilen nachhaltig beeinflussen. Negative Ereignisse, also Ereignisse mit einem hohen Risiko auch für das eigene Handeln, werden außerdem zusätzlich leichter erinnert.

(3) Bestätigungstendenz: Hat man in Bezug auf bestimmte handlungspraktische Kontexte feste Meinungen oder Ideen erreicht, bleibt man in der Regel gerne dabei und lässt sich nur ungern das Gegenteil beweisen. Das führt zu einer stringenten Tendenz, bestätigende Ereignisse eher wahrzunehmen und zu erinnern als widersprechende. Die eigenen Werte strukturieren also die eigene Wahrnehmung.

(4) Repräsentativitätsheuristik: Sind Personen in die handlungspraktischen Kontexte involviert, werden diese häufig anhand einiger zugänglicher Merkmale einer subjektiven Personenkategorie, einem Stereotyp zugeordnet (auch Halo-Effekt genannt). Diesem Stereotyp werden entsprechend Intentionen und Möglichkeiten unterstellt. Beur-

> teilungen von Handlungen oder Erwartungen dieser Person verlaufen eher nach den eigenen Erwartungen an den Stereotyp als nach den realen Äußerungen und Handlungsweisen der Person.

Für die Beurteilung komplexer, risikobehafteter Situationen sind also medial präsente Zahlen und Geschichten, eigene vorgefasste Meinungen und Ideen sowie Stereotype entscheidend. Sie lösen die objektiven Fakten, die empirisch realen Bemühungen und Personen in der Beurteilung ab und prägen vor allem die Wahrnehmung unbekannter Anteile, also der Dunkelfelder und der fehlenden objektiven Zahlen zu Sicherheit.

In den komplexen technischen Debatten lassen sich diese Selbstmanipulationen allerdings kaum erkennen. Es bedarf großer Sachkenntnis und insbesondere auch einer Kenntnis der Agenden und Interessen der Akteure, um die Hintergründe dort zu detektieren und zu bewerten. Für Laien ist das meist unmöglich. Sie werden mit einer entsprechenden Unschärfe leben müssen, solange die Forschung sich nicht um eine Erhellung und laientaugliche Explikation der Dunkelheiten bemüht. Bei allen ethischen Erwägungen sollte man sich entsprechend vorher um maximale Aufklärung und in den Erwägungen selbst um hohe Objektivität bemühen.

4.6 Der Wert der Sicherheit im Kontext Cybercrime

Wir wissen nun also, dass es in unserem Feld der Informationsethik im Kontext von Cybercrime besonders wichtig ist, sich über die Werte und Strukturen im Klaren zu sein, da sich so plausible Szenarien entwickeln lassen, mit denen sich die Komplexität des Problems durchdringen lässt, um bessere Urteile fällen zu können. Wir werden uns daher im folgenden mit den in diesem Feld betroffenen Werten und den Strukturen des Handelns des Strafverfolgers auseinandersetzen. Allerdings werden wir an dieser Stelle vorerst noch einen wichtigen Ausschnitt machen, indem wir zuerst nur die relevante Basisrisiken für die Begründung des Wertes der Sicherheit sowie die Strukturen der Strafverfolgung als Strukturen der Sicherheit aufführen. Die Werte und Strukturen der Freiheit werden wir umfassender im zweiten Teil des Studienbrief aufführen und diskutieren.

4.6.1 Risiken durch Cybercrime

Zuerst müssen wir festhalten, wie „schlimm“ Cybercrime in all seinen Facetten sein kann und wer in welcher Form betroffen sein kann. So bringen wir in Erfahrung, wie intensiv wir von diesem Phänomen betroffen sind, als

wie wichtig wir also die Herstellung von Sicherheit in diesem Fall erachten müssen. Eine Vermessung der Schäden und Risiken ist jedoch leider alles andere als einfach.

4.6.2 Monetäre Risiken

Direkte Schäden

Zunächst lassen sich verschiedene „Ordnungen“ von Schadenshöhen konstatieren. Schäden erster Ordnung sind die unmittelbaren Schäden eines Vorfalls. Hierzu zählen vor allem akute Ausfälle bei Störungsangriffen und die damit zusammenhängenden Verluste, sonst aber vor allem die Kosten der Abwehr des Angriffs und der Herstellung der Continuity der Prozesse. Diese Kosten können bereits erheblich sein, variieren aber sehr stark von Fall zu Fall, abhängig von Kenngrößen wie technischem Outset und technischer Komplexität oder dem Geschäftsprozess in dessen Dependenzen und Kritikalität für weitere Geschäftsprozesse. Schäden erster Ordnung lassen sich allerdings in der Regel gut messen und quantifizieren, da sie direkt anfallen.

Folgeschäden

Schäden zweiter Ordnung sind Schäden, die nach dem Vorfall und auf der Basis der entstandenen Probleme entstehen. Hierzu zählen etwa Kosten wie die weitere technische Bereinigung des Systems, neue technische Sicherheitsmaßnahmen, PR-Maßnahmen zur Minderung eines Rufschadens, direkte Schadensersatzzahlungen oder Anwaltskosten.

Langfristige Schäden

Schäden dritter und vierter Ordnung sind schließlich Schäden, die langfristig auf Basis der Schäden erster und zweiter Ordnung entstehen. Hier sind vor allem mit langfristigen Auswirkungen der Kosten auf die Geschäftsliquidität, die langfristigen Folgen eines Rufschadens, die Angst des Unternehmens vor IT und die damit entstehenden Kosten, weitere Schäden an Kunden und Partnern des Opfers durch die Daten oder durch Analogieschlüsse des Täters oder – im schlimmsten Fall Verdrängung aus Märkten durch konkurrenzorientierte Industriespionage – zu rechnen.

Damit wird andeutungsweise sichtbar, dass Cybervorfälle eine ganze Bandbreite von Schäden über teilweise längere Zeiträume anrichten können. Gleichzeitig lassen sich zwei Dinge erahnen, nämlich zum einen, dass die größten Schäden in den späteren Stadien höherer Ordnung entstehen können und zum anderen, dass gerade diese Schäden nur äußerst schwer abzuschätzen sind. Denn je weiter die Schäden in ihrer Ordnung nach hinten gehen, desto mehr Kausalitäten liegen dazwischen und umso schwerer lassen sie sich mit dem Vorfall in unmittelbare Verbindung bringen.

Sinkt etwa bei einem Unternehmen, das vor einiger Zeit einen Cyberschaden öffentlich gemacht hat, eine Weile danach der Umsatz, lässt sich dies kaum eindeutig auf den Vorfall zurückführen. Es könnte eine Reihe von Faktoren dort eine Rolle spielen. Das Gleiche gilt für viele Fälle von Industriespionage. In einigen Fällen gibt es eindeutige Hinweise. Es wurden Fälle berichtet, bei denen Maschinen peinlich genau bis auf die Seriennummer kopiert wurden. Aber in den meisten anderen Fälle integrieren die Spione das gestohlene Wissen in bestehende Produkte oder mit anderem gestohlenem Wissen, sodass insbesondere bei komplexen Technologien kaum sichtbar ist, ob Teile davon kopiert sind oder nicht.

Hinzu kommt, dass Schäden durch Cybervorfälle auch sehr individuell sein können. Ein in seinem technischen Outset ähnlicher Vorfall kann bei einem Opfer einen moderaten Schaden auslösen, bei einem anderen Opfer einen gigantischen Schaden. Dies macht Extrapolationen von einem Fall auf einen Menge von Fällen sehr schwer. Erst eine größere Zahl kausal eindeutiger Fälle ließe eine präzise Voraussage von Mittelwerten zu. Die lässt sich aber schlicht nicht erstellen.

Diese Unsicherheiten generieren erneut Dunkelräume. Aufgrund dieser Unschärfen lässt sich nämlich nicht genau sagen, wie hoch die Schäden eines Vorfalls sind. Nimmt man nur die Schäden erster und zweiter Ordnung, sind dies – in die Breite gerechnet – meist eher moderate Summen. Das allerdings wird auch allgemein als zu kurz betrachtet. Schäden höherer Ordnung müssen Eingang finden. Also muss man schätzen. Und damit beginnt ein Drama. Denn wenn schon im Schätzen der Dunkelziffern des Detektierens und Messens kreative Freiheiten Schäden erhöhen oder erniedrigen können, gilt dies im Schätzen von Schäden höherer Ordnung umso mehr. Diese Unsicherheiten multiplizieren sich dann mit den Unsicherheiten der Dunkelziffern, sodass also de facto eine dauernde „Raterei“ vorherrscht bei der Bestimmung möglicher gesamtgesellschaftlicher Schäden.

Zusätzlich zu den Problemen, dass Schäden nicht bemerkt oder nicht korrekt eingeschätzt werden, kommt das Problem, dass viele Schäden, selbst wenn sie bemerkt werden, nicht gemeldet werden. Auch dies hat viele Ursachen. Zum einen handelt es sich bei einigen Vorfälle nur um kleine Summen, bei denen sich das Einschalten der Polizei im Einzelfall nicht lohnt. Viele Menschen haben auch den Eindruck, dass ihnen die Polizei ohnehin nicht helfen kann, wenn es um Cyberverbrechen geht – ein Eindruck, der nicht ganz unberechtigt ist, wie wir im Laufe dieses Briefes noch

sehen werden. Davon abgesehen aber gibt es noch eine große Klasse von Opfern, die nicht als Opfer bekannt werden möchten. Dies gilt natürlich vor allem für Unternehmen, die Rufschäden zu befürchten haben oder die sogar einen Verlust von Kundendaten anmelden müssten. Der erste Fall des Rufschadens muss natürlich nicht eintreten, wenn man sich vertrauensvoll an die Polizei wenden kann. Allerdings ist das Risiko einer versehentlichen oder absichtlichen Veröffentlichung bei einer Meldung eben doch größer als ohne Meldung. Bei großen Unternehmen, deren Geschäft auf hohem Vertrauen beruht, wie etwa Banken, können die Schäden dann als so gravierend eingeschätzt werden, dass man selbst bei den größten Beteuerungen immer noch Abstand von einer Meldung nimmt. Meldungen an stärker vertrauensvolle Institutionen wie die BAFIN dagegen sind etwas häufiger. Der zweite Fall eines Verlusts von Kundendaten oder anlegerrelevanten Assets wiegt sogar noch schwerer. Hier sind unmittelbare Kosten zweiter Ordnung durch Klagen der indirekt Betroffenen zu erwarten, die zum Teil große Beträge erreichen können.

Meldungen werde nicht gemacht

Die Meldepraxis der Unternehmen ist damit also – wenig überraschend – ausnehmend schlecht. Man hat allgemein den Eindruck, dass so etwas weit eher schadet als hilft. In der Folge ist auch hier ein Dunkelfeld, das zu kreativen Auslegungen einlädt.

Meldung an Antiviren Hersteller

Eine andere Institution für Meldungen wären die Hersteller von Antiviren-Produkten. Diese Unternehmen verfügen durch ihre Kundenkontakte natürlich zum Teil auch über einen Einblick in Schäden. Allerdings ist dieser Blick geprägt von einem eher sehr kleinen Segment ausgewählter Kunden und wird von dort aus meist unfundiert direkt extrapoliert, was oft zu vermutlich recht utopischen Vorstellungen von Schäden führt.

Die schlechte Sichtbarkeit des Phänomens in vielen Bereichen ist ein schwieriges Problem. Vor allem die in einer rein qualitativen Risikoabschätzung eher weniger gefährlichen Cyberverbrechen sind sichtbar, während die gefährlicheren Verbrechen deutlich unsichtbarer sind. Dies hatte eine unangenehme Nebenwirkung. Da nämlich die Bekämpfung von Cybercrime eine komplexe und teure und – wie wir hier ja diskutieren – umstrittene Angelegenheit ist, tendieren die Entscheider in diesem Feld zu Entscheidungen mit niedrigen Risiken für die Richtigkeit der Entscheidung selbst. Dies sind in der Regel grundlegend effektive, aber eher kostengünstige und wenig effiziente Maßnahmen gegen die sichtbarsten Verbrechen. Etwas sarkastisch ausgedrückt führt uns das also in die Situation, dass wir in diesem Feld

dazu tendieren, die irrelevantesten Verbrechen mit den eher billigen Maßnahmen zu bekämpfen, was aus einer strategischen Perspektive hohe und zahlreiche Restrisiken übrig lässt. Die sind wieder unsichtbar, von daher kein Risiko für die Entscheider, aber dennoch gesellschaftliche Risiken.

Dies ist bereits ein wichtiges Thema für den gesellschaftlichen Diskurs, das allerdings noch weit zu wenig Aufmerksamkeit erfährt. Es gibt aber noch ein wichtiges Element am Problem der Sichtbarkeit, das sich deutlich auf alle im Weiteren zu besprechenden gesellschaftlichen Probleme und Debatten auswirkt. Die schlechte Sichtbarkeit, die Dunkelheit der Dunkelfelder und die schlechte Messbarkeit von Sicherheit werden von den Akteuren der gesellschaftlichen Debatten regelmäßig „missbraucht“, um Argumente in die eine oder andere Richtung zu dramatisieren oder zu entschärfen. Dieses Problem der Unsachlichkeit vieler Debatten ist ein übergreifendes Metathema, dem leider noch zu wenig Aufmerksamkeit gewidmet wird. Zu viele Akteure werden als neutrale Vermittler wahrgenommen, die dies in Wirklichkeit nicht sind und nicht sein können.

Ein weiteres bislang noch zu wenig diskutiertes Problem ist das Verhältnis der direkten Kosten zu den indirekten Kosten. Hier haben inzwischen mehrere Untersuchungen herausgefunden, dass die indirekten Kosten der Bekämpfung von Cybercrime und der Beseitigung seiner Folgen ein Zehnfaches bis – in einigen Fällen – ein Hundertfaches der Kosten der eigentlichen Verbrechen betragen. Dies mag zwar notwendig erscheinen, da ohne die Gegenmaßnahmen ein Ausufern der Verbrechen und ihrer Folgen angenommen werden könnte, es muss aber dennoch thematisiert werden, da das Verhältnis direkte zu indirekte Kosten für alle anderen Verbrechensformen gänzlich anders ausfällt. Die indirekten Kosten liegen hier meist weit unter den direkten Kosten.

Anderson beschreibt dieses Phänomen wie folgt:

„Traditional frauds such as tax and welfare fraud cost each of us as citizens a few hundred pounds/euros/dollars a year. With such crimes, the costs of defences, and of subsequent enforcement, are much less than the amounts stolen. Transitional frauds such as payment card fraud cost each of us as citizens a few tens of pounds/euros/dollars a year. Online payment card fraud, for example, typically runs at 30 basis points, or 0.3 % of the turnover of e-commerce_rms. Defence costs are broadly comparable with actual losses, but the indirect costs of business foregone because of the fear of fraud, both by consumers and by merchants, are several times higher. The

new cyber-frauds such as fake antivirus net their perpetrators relatively small sums, with common scams pulling in tens of cents/pence per year per head of population. In total, cyber-crooks' earnings might amount to a couple of dollars per citizen per year. But the indirect costs and defence costs are very substantial – at least ten times that. The cleanup costs faced by users (whether personal or corporate) are the largest single component; owners of infected PCs may have to spend hundreds of dollars, while the average cost to each of us as citizens runs in the low tens of dollars per year. The costs of antivirus (to both individuals and businesses) and the cost of patching (mostly to businesses) are also significant at a few dollars a year each." (1, S. 25)

Es scheint also, als seien unsere Gegenmaßnahmen nicht sonderlich kosteneffizient. Dies wirft die dreiseitige Frage auf, (1) ob es an einer überzogenen Wahrnehmung des Problems liegt, dass wir also einfach zu viel Aufregung betreiben, (2) ob dieses Missverhältnis durch die höhere Effizienz des Cybercrime im Verhältnis zu konventionellen Verbrechen zustande kommt, sozusagen „gegen-proportional" abbildet, dass hier wesentlich mehr getan werden muss, oder (3) ob in den Wahrnehmungen der Disproportion infolge der schlechten Sichtbarkeit der höher riskanten Verbrechensformen diese ausgeblendet wurden, sodass im Grunde eine Proportionalität besteht, die aufgrund der Auswahl des Referenzraumes der Studien nur nicht erkennbar ist.

Die Antwort auf diese Frage ist noch offen. Es gibt bereits Indikatoren dafür, dass alle drei Faktoren eine Rolle spielen. Übergreifend wird hier sichtbar, dass die Risiken und die Effizienzen von Sicherheitsmaßnahmen in keiner Weise eine abgeschlossene oder mit festen Größen operierende Debatte darstellen. Klar ist, dass einige Kriminalitätsformen deutlich größere Schäden verursachen als andere. So werden die Schäden durch Industriespionage oder Finanzmarktmanipulationen die Schäden durch kleine Cyberbetrügereien absolut in den Schatten stellen. Aber Zahlen sind für diese Fälle eben nur schwer zu erheben.

Wir werden also die Debatte der Kosten auch nicht mit der Illusion konkreter Zahlen abschließen, indem wir einige der aktuell kursierenden Berichte nacherzählen, sondern diese mit den Bemerkungen zu den diversen Unwägbarkeiten und Problemen bei der Vermessung an dieser Stelle beenden. Die konkreten Zahlen können den je aktuellen Berichten etwa des BKA oder der Industriekammern entnommen werden.

Kontrollaufgabe 4.1: Indirekte Kosten

Was sind indirekte Kosten und wie würden Sie die Angemessenheit dieser Kosten beurteilen?

K

4.6.3 Nicht-monetäre Risiken

Zusätzlich zu den direkten und indirekten Kosten des Cybercrime müssen nun jedoch noch weitere Risiken berücksichtigt werden. Denn auch wenn die meisten Formen des Cybercrime auf Geld ausgerichtet sind, gilt dies nicht für alle. Zudem generieren viele der monetär ausgerichteten Kriminalitätsformen noch weitere, nicht monetäre Schäden.

Cyberterror

Ein wichtiges Risiko im Grenzbereich zum Cyberwar ist der sogenannte „Cyberterror“. In diesem Szenario wird davon ausgegangen, dass es Terroristen gelingt, signifikante Fähigkeiten des Hacking zu entwickeln, um dann terroristische Angriffe auf besonders kritische Infrastrukturen oder Maschinen mit „Megadeath“-Optionen zu fahren. Aber das strategische Kalkül und die taktischen Bedingungen von Terroristen vertragen sich nicht besonders gut mit den dafür notwendigen Rahmenbedingungen. Denn Cyberangriffe auf Einzelziele mit Terrorwirkung sind zwar eingeschränkt möglich, aber ungemein aufwändig. Für diese Art Angriffe müssten Angreifer entweder phänomenal Glück haben oder über umfangreiche Ressourcen, einen Nachrichtendienst, Wissenschaftler, Fachexperten, Testanlagen und viel Zeit verfügen. Das meiste davon wird für Terroristen nicht zutreffen. Sie sind strukturell auf Guerilla-Taktiken angewiesen, die ihnen ein zu umständliches, umfangreiches Vorgehen systematisch verwehren. Diese Situation kann sich ändern, wenn erst einmal viele Militärs über sehr gute Hacker verfügen und entsprechend viele Fachkräfte und vielleicht auch Angriffe auf den Markt kommen. Auch entwickelt sich gerade ein Söldnermarkt, der diese Angriffe herstellen und verkaufen könnte. Aber selbst dann werden solche Angriffe viel Customizing und Entwicklungsaufwand benötigen und alles andere als trivial sein.

Nichtsdestotrotz sind einige der Worst-Case-Szenarien in diesem Bereich nicht als völlig unwahrscheinlich zu entwerten, wobei die Schäden außerordentlich groß sein können. Eine Bewertung bleibt durch die hohen Unsicherheiten jedoch schwierig.

Politischer Aktivismus

Ein weiteres Phänomen krimineller Aktivitäten im Cyberspace stellt der illegale politische Aktivismus dar. Aktivismus ist inzwischen ein sehr gängiges Phänomen im Internet. Die Gründe dafür liegen auf der Hand. Aktivisten können sich auf diese Weise Aufmerksamkeit verschaffen, können medial wirken, sie können ihre Adressaten meist direkt schädigen und ansprechen, sie können über Grenzen hinweg agieren, und sie können erneut Anonymität und Pseudonymität nutzen, um möglichen strafrechtlichen Konsequenzen besser zu entgehen. Entsprechend häufig sehen wir inzwischen bei allen möglichen politischen Phänomenen eigene begleitende politische Komponenten im Internet. Jede Variante militärischen Konflikts, jede politische Aufregung wird durch umfangreiche Aktivitäten im Netz begleitet. Dabei können allerdings nicht einfache Kommentare oder Webseiten bereits als illegal gewertet werden. Es muss als eine wichtige Voraussetzung für eine entsprechende Bewertung eine kriminelle Beeinträchtigung anderer vorliegen. Dies ist etwa dann der Fall, wenn legitime Webseiten einer Partei gehackt und wenn deren Inhalte ausgetauscht werden. Dies ist eine sehr gängige Form des politischen Aktivismus im Netz. Man sieht häufig, wie bereits erwähnt wurde, dass etwa politische Gegner mit Hitlerbärten ausgestattet werden oder dass politische Kampfnachrichten auf die Webseiten der Gegner gebracht werden. Dies sind allerdings auch keine besonders gravierenden kriminellen Aktivitäten. Die realen monetären wie nicht-monetären Schäden sind eher gering, wobei entsprechend geringe Schäden im Kontext von politischen Demonstrationen zwar immer noch illegal, aber eben nicht dramatisch und im Kontext der Bekämpfung möglicherweise größeren Unheils moralisch unter Umständen sogar legitim. Bewertungen müssen hier also immer sehr fallspezifisch ausfallen.

Kriminelle Meinungsmanipulation

Kriminelle können auch ein Interesse ausbilden, das politische Wissen und Meinen im Internet zu manipulieren. Dies kann indirekt monetäre Anreize haben, wenn sich etwa mit bestimmten Fehlinformationen viel Geld machen lässt, kann aber auch politisch motiviert sein, wenn bestimmte Meinungen nicht als tragfähig oder tolerabel empfunden werden. In diesen Fällen können Akteure es auf sich nehmen, im Web 2.0 Propaganda zu platzieren, öffentliches Wissen und Meinen zu infiltrieren, politische Diskussionen zu manipulieren, Themen zu setzen oder zu fingieren und Ähnliches mehr. So wurden etwa bereits kleinere Abstimmung im Rahmen einer digitalisierten Öffentlichkeit angegriffen. In den meisten Fällen hieß es dabei, dass es sich

um politischen Protest oder um Aktivisten handelt. De facto allerdings weiß man nie genau, ob es jetzt tatsächlich nur ein einfacher politischer Protest war oder eine durch einen Nachrichtendienst fingierte Aktion. Aber nicht nur diese direkten Wahlen und Abstimmungsprozesse sind verwundbar. Auch die politische Kommunikation ist es geworden. Sie ist zunehmend ins Netz verlagert. Blogs, Twitter, Facebook und ähnliche Werkzeug des Web 2.0 spielen heutzutage eine ausnehmend wichtige Rolle für die politische Meinungsfindung. Dabei sind sie allerdings alles andere als neutral und unabhängig. Natürlich wird dies von den Apologeten der Internetfreiheit nicht gerne gesehen. Aber die absolute Freiheit des Internets und des Web 2.0 – in den Augen einiger Befürworter ein entscheidender Vorteil – ist politisch gesehen schwierig. Denn diese Art von Freiheit ist nicht die politische Freiheit. Sie ist nicht egalitär, sondern sie bevorzugt denjenigen, der mit den meisten Ressourcen und dem besten Know-how einsteigt. Es ist eine naturrechtliche Freiheit. Dadurch sind diese Kommunikationswege auch nicht besonders vertrauenswürdig. Man weiß unter Umständen nicht, wer bestimmte Diskussionen antreibt, wer in den Diskursen alles mitredet und mit welchen Interessen.

Strategische Langzeitschäden und Wissensproliferation

Ein weiteres Problem kann entstehen, wenn bestimmte Kriminalitätsformen besonders lange mit hoher Effizienz durchgeführt werden. Dies gilt insbesondere für Industriespionage. Da in der späteren Ausbeutung des gestohlenen Wissens kompetitive Industrien ausgebildet werden und methodisches Produktionswissen bei einem andernfalls benachteiligten Konkurrenten entstehen, werden also in dieser Variante der Kriminalität nicht nur konkrete Forschungsergebnisse entwendet, um eventuell in Konkurrenzprodukte zu erscheinen. Man zieht auch eine ganze Wirtschaft groß, die der eigenen sehr ähnlich und in einigen Strukturen durch die Modalitäten der günstigen Akquise von Wissen sogar überlegen ist. Damit können also volkswirtschaftliche Folgeschäden entstehen, die die konkreten Schäden leicht in den Schatten stellen.

Zudem muss beachtet werden, dass die Angreiferseite bei einem ungehinderten Operieren ihre Fähigkeiten immer weiter ausbaut, also immer besser und heterogener wird, so dass sie auch bessere Ziele angreifen kann, immer stärker unsichtbar wird und entsprechend größere Schäden generiert. In diesem Kontext muss auch beachtet werden, dass unter Umständen auch eine Weiterverbreitung, also eine Proliferation der Offensivkenntnisse statt-

finden kann. Dies ist in der Vergangenheit bereits öfter passiert und hatte verschiedene, oft schlechte Konsequenzen. Neue Angreifer haben sich formiert und die Zahl der Angriffe erhöht, dabei aber auch das Zielspektrum verändert, so dass plötzlich vollkommen neue Gefahrenbereiche entstanden. Zudem können unter solchen Bedingungen auch neue arbeitsteilige Organisationsformen der Kriminalität entstehen, die eine bedeutend höhere Effizienz nach sich ziehen.

Eskalationen

Ein weniger, aber nicht vollkommen unwahrscheinliches Szenario könnte auch in einer Eskalation einer kriminellen Aktivität bestehen. So ist durchaus denkbar, dass cyberkriminelle Aktivitäten im Kontext eines militärischen oder vor-militärischen Konflikts absichtlich oder unabsichtlich als militärische Aktivitäten fehlgedeutet werden und so zu einer Katalysierung des Konflikts beitragen. Dieses Szenario wird allerdings nur in Ausnahmefällen Anwendung finden, nämlich im Krieg, in dem ohnehin ein anderes Wertegefüge zu berücksichtigen sein wird.

Vertrauensverluste

Eine weitere Spätfolge können Vertrauensverluste sein. Sind mehrfach Probleme mit digitalen Medien und Kommunikationen aufgetreten – im politischen wie im wirtschaftlichen Kontext – so werden sich die Nutzer dieser Medien zum Teil zurückziehen, was seinerseits zu einem Verlust an politischer oder kulturelle Teilhabe oder zu wirtschaftlichen Verlusten führen kann, die dann als weitere materielle wie immatrielle Kollateralschäden anzusetzen sind.

4.6.4 Bewertung der Risiken

Eine Bewertung dieser Risiken fällt nun nicht leicht. Wir wissen nach wie vor wenig Konkretes über dieses Phänomen – auch wenn wir es jeden Tag beobachten. Übergreifend müssen wir Cybercrime aber als ein äußerst attraktives Verbrechen bewerten, das mit Sicherheit noch viele weitere Angreifer und Angriffe generieren wird. Die Gewinne sind mitunter sehr hoch, währen die Kosten verhältnismäßig moderat und die Risiken zur Entdeckung bei einer ausreichend kenntnisreichen Vorgehensweise sehr niedrig sind. Zudem ist diese Form des Verbrechens ein bequemes Schreibtischverbrechen, bei dem man sich nicht in die physischen Gefahren echter Einbrüche oder Erpressungen begeben muss. Dies macht diese Form der

Kriminalität auch für viele Charaktere attraktiv, die sonst aufgrund dieser physischen Dimensionen von Verbrechen zurückschrecken würden. Da diese Attraktivitätsfaktoren sehr tief in den Strukturen unserer Informationsgesellschaften angelegt sind, ist davon auszugehen, dass sie auch in nächster Zeit nicht signifikant verändert werden können, sodass also diese Variante des Verbrechens weiterhin attraktiv bleibt und hohe Zuwachsraten erfährt. Dabei muss vor allem damit gerechnet werden, dass die Angreifer stärker auf gezielte Aktivitäten umsteigen und dass stärker organisierte und talentierte Akteure in nächster Zeit das Feld betreten werden. Außerdem ist auch mit einem quantitativen Anwachsen zu rechnen. Insbesondere aufgrund dieser dynamischen und zukunftsgerichteten Faktoren ist Cybercrime also durchaus ein ernstzunehmendes Phänomen.

4.7 Strukturen der Sicherheit im Kontext Cybercrime

Neben den unmittelbare und mittelbaren Risiken ist noch eine Reihe weiterer Merkmale des Cybercrime zu berücksichtigen, da sie dafür verantwortlich sind, dass die Strafverfolgung auf ethisch schwierige Modalitäten gezwungen wird. Ein Verständnis dieser Merkmale ist also informationsethisch ebenfalls relevant, um die Bedingungen des Handelns in diesem Feld und davon ausgehend die Möglichkeiten für Alternativen zu bewerten. Sehen wir uns also einmal an, was wir denn eigentlich alles wissen müssen, damit wir eine Strafverfolgung überhaupt ansetzen können.

4.7.1 Strukturmerkmal Identität

Ein Strafverfolger muss zur Strafverfolgung einmal einen Verbrecher identifizieren, einen Akteur, der verantwortlich gemacht und verhaftet werden kann. Ein Verbrechen muss personalisiert werden können. Ein erstes Indiz zur Identifikation wäre die Maschine, von der ein Angriff ausgegangen ist. Dies ist insbesondere für die Forensik immer der erste und wichtigste Anhaltspunkt. Man muss feststellen können, auf welcher Maschine ein Angriff abgesetzt wurde. Dies ist bereits ungemein schwierig. Wir können zwei Varianten unterscheiden: Online-Angriffe und Offline-Angriffe. Bei Online-Angriffen hat man das Problem, dass man hier direkt mit der Kernidee des Internets konfrontiert wird. Die Idee des Internets war eben eine über mehrere Punkte verteilte Kommunikation, sodass man im Fall eines Atomkrieges stärker widerstandsfähige Kommunikationsnetzwerke hat.

Identifikation der Angriffsmaschine

Das war die ursprüngliche Idee des Internets damals in den Händen der DARPA. Genau dieses Prinzip einer über viele Punkte weitergeleite-

Angreifer wählt eigenen Pfad durchs Internet

ten, fragmentierten Kommunikation macht nun allerdings eine Online-Identifikation ungeheuer schwierig. Denn ein geschickter Angreifer kann die Pfade, die sein Angriff bis zum Ziel über das Internet nimmt, steuern und beeinflussen. Zum einen kann er dabei seine Spuren verwischen. Er kann die Informationen über die Punkte, die der Angriff auf dem Weg zurückgelegt hat, auslöschen. Dazu muss er nur entsprechende Anweisungen in seinen Angriff inkorporiert oder einige der Wegpunkte selbst angegriffen haben. Meist ist dies aber gar nicht notwendig, da die verschiedenen Wegpunkte eines solchen Angriffs diese Informationen ohnehin nur für einige Sekunden oder wenige Minuten speichern. Danach werden diese Informationen nicht mehr benötigt. Der Weg der Information ist abgeschlossen, sodass die Speicherplätze dafür wieder freigegeben und überschrieben werden. Die Information ist dann unwiederbringlich verloren. Außerdem kann ein geschickter Angreifer noch verschiedene andere Tricks benutzen, um eine Kommunikation so aussehen zu lassen, als käme sie von einer bestimmten Maschine, während sie in Wirklichkeit von einer ganz anderen kommt. Hier ist das Arsenal der potentiellen Tricks vielfältig. Sich einfach in andere Maschinen einzuhacken und von dort aus zu agieren, ist ein einfaches Beispiel.

Informationen zwischen Maschinen gehen verloren

Hier kommt also ein herausragend wichtiges Kernmerkmal des Cybercrime als Bedingung des kriminalistischen Arbeitens zum Tragen, nämlich der Umstand, dass jede computervermittelte Kommunikation oder Interaktivität nicht Face-2-Face ist, sondern Interface-2-Interface. Sie findet also nicht von Angesicht zu Angesicht statt, sondern von Rechner zu Rechner. Dadurch kommt ein „Man-Machine-Gap“ zum Tragen, eine Lücke zwischen dem menschlichen Akteur und der einen Angriff ausführenden Maschine. Diese Lücke kann mit technischen Maßnahmen nicht überbrückt werden und schafft so eine 100 %ige Sicherheit gegen technische Rückverfolgung, bei entsprechenden taktischen Vorsichtsmaßnahmen (wie etwa nicht von zu Hause aus anzugreifen). Dies ist das Element der Anonymität, das hier das erste Mal in Erscheinung tritt. Aber auch verschiedene andere Strukturen in der IT und besonders im Internet ermöglichen Anonymität.

Dabei lassen sich verschiedene Stufen von Identität auseinanderhalten, die anonymisiert werden können:

1. Personale Identität: Hiermit ist die konkrete Person gemeint, die hinter einem Angriff steckt.

2. Institutionale Identität: Dies ist die Organisation, der ein Angreifer möglicherweise zugehört.

3. Nationale Identität: Damit ist angegeben, welcher Nationalität der Angreifer angehört.

4. Kontextuelle Identität: Dies ist eine Variante der Identität, bei der man eine Angreiferidentität über die Kontexte des Angriffs wie Art des Schadens, Ziel, vermeintliche Motivation des Angreifers und ähnliche Dinge festzumachen versucht

5. Technische Identität: Hiermit ist die technische Identität der vom Angreifer benutzten Angriffswege und Angriffswerkzeuge gemeint. Viele dieser Technologien haben eindeutige Orte oder Kennzeichnungen, sodass man hier eine eigene Identität verorten kann, die sich unter Umständen auf die personale oder institutionale Identität abbilden lassen.

All diese Identitätsvarianten können nun bei IT- und Internet-basierten Angriffen gut umgangen werden.

- Personale und institutionale Identität: Diese Identitäten sind bereits gut geschützt durch den Abstand zwischen Tastatur und Fingern, lassen sich aber durch weitere taktische Maßnahmen noch besser schützen. Wichtig ist hier vor allem eine Entkopplung der technischen Identität von der personalen oder institutionalen Identität. So wird eine weitere Anonymisierung etwa stattfinden, indem man keine eindeutig identifizierbaren oder nur sehr flüchtig und unsicher identifizierbaren technischen Werkzeuge und Wege nutzt und indem der „Arbeitsplatz“ möglichst weit von der personalen und institutionalen Identität entfernt liegt.

- Nationale Identität: Diese Identität ist vielen Angreifern egal, da viele Länder nicht in der Lage oder nicht interessiert sind, Cybercrime zu bekämpfen. Es ist aber dennoch immer hilfreich, sie doch zu tarnen, da so Eskalationen durch externe Anfragen an die eigene Regierungen vermieden werden, die ihrerseits zu einem verschärften Bewusstsein gegenüber Cyberrisiken und einem härteren Vorgehen führen könnten. Die nationale Identität lässt sich taktisch anonymisieren durch ein Operieren aus dem Ausland oder technisch durch eine hinreichend effiziente und vielschichtige Umleitung über das Ausland.

- Kontextuelle Identität: Die kontextuelle Identität ist seit einiger Zeit Gegenstand intensiver Überlegungen und Anstrengungen. Viele Strafverfolger und forensische Dienstleister bauen darauf, dass Angreifer sich ein Stück weit über ihre Fähigkeiten und Interessen und ähnliche Dinge verraten. So werden etwa Elemente wie das Ziel, dessen Ausbeutung, die Qualität und die Dauer des Angriffs, verwendete Techniken und Programmierstile genutzt, um typische Akteure dahinter zu mutmaßen. Anonymität ist hier nicht so leicht herstellbar, denn dem Opfer steht immer auch ein Mindestsatz eigener Informationen zur Verfügung, die der Angreifer nicht vollständig kontrollieren kann. Hier kann jedoch Pseudonymität angebracht werden. Diese Variante von Anonymität werden wir gleich noch genauer besprechen.

- Technische Identität: Die technische Identität lässt sich weitgehend anonymisieren und verschleiern. Man kann falsche oder irrelevante Adressen nutzen („Briefkastenfirmen“ sozusagen), andere Merkmale umgehen oder umschreiben. Allerdings muss man sich als Angreifer gut mit den verschiedenen Charakteristiken auskennen, die zu solch einer Identität gehören. Das Problem für den Angreifer ist hier, dass diese Liste theoretisch sehr groß sein kann. Man hinterlässt, besonders bei mehreren Angriffen, auch viele Datenspuren. Können Strafverfolger alle Spuren sichern, so könnten über Big Data-Analysen Querverbindungen gefunden werden, die aus dem Heer der Spuren konkrete Hinweise auf personale und institutionale Identität geben. Dies ist aktuell ein großer und wichtiger Trend in der Identitfikation von digitalen Missetätern. Prinzipiell ist aber auch eine weitgehende Kontrolle durchaus möglich. Big Data-Analysen sind zudem anfällig dafür, mit Falschinformationen geflutet und auf falsche Schlüsse gebracht zu werden. Dies ist ein Vektor, der sich nur schwer abstellen lässt und der von Angreifer vermutlich leicht zu entwickeln sein wird. Zudem kann auch hier Pseudonymisierung eingesetzt werden.

Damit ist der nächste wichtige Punkt bereits angesprochen.

Der Man-Machine-Gap ebenso wie viele andere Strukturen, die digitalen Identitätswandel ermöglichen, haben noch eine andere wichtige Ausprägung, die nicht nur für die Vermeidung der Erkennung, sondern auch für die konkrete Durchführung von Verbrechen äußerst relevant ist: Sie ermöglichen Pseudonymität. Pseudonymität bedeutet, dass der Angreifer nicht versucht, seine Identität auszulöschen, sondern dass er anstelle seiner eigenen Identität eine mehr oder weniger gut gefälschte Identität anlegt

und von dieser aus agiert. Auch dafür bieten digitale Technologien zahlreiche Ansatzpunkte. Man kann Profile erfinden, E-Mail-Absender gestalten, Webseiten fälschen und viele andere Indikatoren fabrizieren, die man im „echten“ Leben oft als genuine Ausdrücke einer Identität akzeptieren würde.

Im Rahmen der Strafverfolgung kann Pseudonymität genutzt werden, um potentielle Ermittler auf eine falsche Fährte zu locken. Insbesondere bei kontext- oder Big-Data-basierten Analysen wird dies leicht möglich und zielführend sein, da diesen Mitteln in diesen Fällen oft viel Gewicht eingeräumt wird und da gefälschte Spuren von echten Spuren oft nur schwer zu unterscheiden sind – besonders, wenn der Angreifer die Analysten und ihre Verfahren kennt. Hier kommt eben der bereits im letzten Studienbrief besprochene apologische Charakter von Datenspuren zum Tragen.

Aber Pseudonymität ist nicht nur günstig, um seinen Verfolgern zu entkommen. Sie bietet auch die Basis für die meisten Varianten des Computerbetrugs. In dieser Kategorie Straftaten nehmen Angreifer eine Identität an, mit deren Hilfe sie eine vertrauenserweckende und finanziell ausbeutbare Verbindung zu einem Opfer aufbauen können. Sie geben sich als Bank aus und fordern dringend PINs und TANs, als Freund oder Verwandter in Not in Übersee oder als wunderschöne junge Frau, die sich nach ältlichen, dicken Männern sehnt.

In vielen Fällen funktioniert diese Betrugsvariante recht gut. Wir werden später noch einige Modelle genauer kennenlernen.

Strukturmerkmal Internationalität

Nun kommt noch ein weiteres Problem hinzu. Um einen Angriffspfad über verschiedenen Rechner zurückzuverfolgen, benötigt man in der Regel Zugang zu den Zwischensystemen, den sogenannten Proxys. Diese gehören aber anderen, unschuldigen Personen, unter Umständen sogar anderen Jurisdiktionen. Man darf sich also nicht ohne weiteres Zugriff darauf verschaffen. Eine gerichtliche Genehmigung dauert in der Regel allerdings wesentlich länger, als Datenspuren halten. Neben den technischen müssen also auch rechtliche und politische Probleme überwunden werden – weitere Dimensionen für ethische Erwägungen in direkter wie in indirekter Weise.

Ein weiteres wichtiges Merkmal ist also die Internationalität und damit die

Transterritorialität des Angriffsmediums Internets. Hier hat der Strafverfolger vor allem das Problem, über unterschiedliche Werte- und Rechtskulturen hinweg agieren zu müssen. Das Internet spannt sich inzwischen über den gesamten Globus und durch alle Länder. Angreifer können dies bei Internet-basierten Angriffen gut nutzen, um eine große Schlagdistanz zu erreichen, um also an einem ganz anderen Ort zuzuschlagen als der, an dem sie sich befinden. Dies ist einmal interessant, um neuen Arten von Opfern zu adressieren. Die nigerianischen 419-Betrüger etwa würden vermutlich allein in Nigeria kaum etwas verdienen. Erst die Möglichkeit, sich nach Europa oder Amerika auszubreiten eröffnet ihnen die Option, in diesen reicheren und besser vernetzten Gegenden Betrugsopfer zu suchen und auszunehmen. Dann aber entzieht die große Schlagdistanz den Angreifer auch des Zugriffs der Strafverfolger aus dem Land seines Opfers. Hier kommt nun der Aspekt der Transterritorialität zum Tragen. Der Begriff des Territoriums umreißt in der Regel einen Rechtsraum. Cybercrime erstreckt sich allerdings oft über mehrere Territorien, sodass also für eine rechtlich saubere Rückverfolgung des Verbrechens verschiedenste Rechtskontexte berücksichtigt werden müssen. Zudem muss hier auch berücksichtigt werden, dass transterritoriale Zugriffe auf Kriminellen ebenfalls schwer sind und vorheriger Verhandlungen und Abkommen bedürfen. Selbst wenn man also in der Lage, transterritorial zu identifizieren, ist man noch lange nicht in der Lage, auch transterritorial zu agieren und zu verhaften.

Dies hat in der Vergangenheit bereits zu vielen Schwierigkeiten geführt und wird sich auch in Zukunft nicht leicht beheben lassen. Strafverfolger benötigen eine enge transterritoriale Kooperation mit anderen Strafverfolgungsbehörden im Ausland auf einer sicheren rechtlichen Basis, um schnell agieren zu können, denn Datenspuren sind – wie bereits erwähnt – recht flüchtig und schnell wieder überschrieben oder nicht mehr auffindbar.

Angreifer kennen diese Problematik nun jedoch genau und leiten daher ihre Angriffe oft gerade über Länder, die keine Kooperationen mit anderen eingehen können oder eingehen wollen. Man kann diese Lücken überbrücken, indem man versucht, sich durchzuhacken, aber das ist in einem rechtlichen Graubereich und nicht unbedingt eine saubere Ermittlungspraxis. Nachrichtendienste können dies tun (und tun es), Polizeien aber kaum, da so kein gerichtlich verwertbares Material erhalten wird. Nur zu Ermittlungszwecken ist es weiter nutzbar. Vielen Polizeien fehlen aber auch einfach die Möglichkeiten, um solche Aktivitäten durchzuführen.

Strukturmerkmale Relative Effizienz

Warum sind so einfache Betrugsversuche wie die 419-Scams aus Nigeria eigentlich noch so ein persistentes Phänomen, wenn nur ein geringer Prozentsatz Opfer auf diese Angriffe hereinfällt? Die Antwort auf diese Frage liegt in der hohen Skalierbarkeit der Angriffe. Ein 419-Scam wie der oben abgebildete kann schon über einfache Strukturen an viele Hunderte Adressen gehen. Mit automatisierten Verfahren, die den Adressraum des Absendens und die Bandbreite erhöhen und Email-Adressen bereitstellen, können sogar Millionen von Opfern gleichzeitig kontaktiert werden. Dann ist klar, dass selbst kleine Ausbeuten einen guten Return on Invest liefern. Wir können vier Varianten von Skalierbarkeit unterscheiden:

1. Massenhafte Anbringung: Wie eben skizziert können Cyberangriffe oft massenhaft gleichzeitig verwendet werden.

2. Wiederholte Anbringung: Eine andere Variante sendet Wellen von Cyberangriffe an Opfer, was mit den gleichen Basistechnologien aus in der Regel recht einfache Art und Weise geschehen kann.

3. Variabilität von Angriffen: Eine dritte Variante der guten Skalierbarkeit betrifft nun nicht mehr die vielfache Anbringung, sondern die Heterogenisierung der Angriffe selbst. Diese Heterogenisierung ist eine wichtige Maßnahme, da – wie im letzten Studienbrief erklärt wurde – viele Sensoren trainieren können, Angriffe zu entdecken. Um den Angriff dann noch weiter nutzen zu können, muss man ihn variieren können. Auch das kann allerdings in der Regel leicht und automatisiert erfolgen, sodass sich also auch hier eine gute Skalierung ergibt. Ein einmal entwickelter Angriff kann leicht wiederverwendet und recycled werden.

4. Ausbeutung des Zugriffs: Eine weitere Option der Skalierung findet sich in der Ausbeutung des Zugriffs. Angreifer, die einmal auf ein System zugreifen können, können dies häufig in „kritischer“ Art und Weise tun, also recht vollständig. In diesen Fällen bemühen sich Angreifer folgend oft, nicht nur die spezifische Information abzugreifen, für die sie gekommen sind. Sie nehmen in der Regel alles mit, was auch nur entfernt nutzbar erscheint. Auch auf diese Weise skalieren also Cyberangriffe recht gut.

Die hohe Skalierbarkeit ist ein wichtiger Nutzen-Faktor des Cybercrime und für die dynamische Szenarioentwicklung wichtig.

K

Kontrollaufgabe 4.2: Strukturmerkmale

Nennen Sie die typisches Strukturmerkmale?

Es gibt zudem auch in vielen taktischen Belangen eine grundlegende Asymmetrie zwischen Offensive und Defensive. Cybersecurity wird von der Offensive dominiert. Der Angreifer ist immer in einer besseren Position als der Verteidiger. Er hat:

1. die Initiative als Auswahl des Ortes, der Zeit und der Mittel des Angriffs;
2. ein geringes Risiko bei Versagen;
3. geringe Menge Code, die er kontrollieren muss;
4. gute Kenntnisse über den Code;
5. gute Möglichkeiten der Kommunikation und Koordination der eigenen Kräfte;
6. eine bessere Kenntnis der Situation;
7. Möglichkeiten für schnelle Entscheidungen.

Dagegen hat der Verteidiger:

1. keine Initiative;
2. muss alles immer gegen jeden Angriff verteidigen;
3. hohes Risiko bei Versagen;
4. große Mengen Code, die er kontrollieren muss;
5. meist schlechte Kenntnisse des Codes, den er verteidigen muss;
6. eher schlechte Möglichkeiten der Kommunikation und Koordination;
7. kaum Kenntnis der Angriffssituation und
8. schlechtere Entscheidungsoptionen.

Die einzigen Vorteile eines Verteidigers sind ein besseres Wissen über das eigene System (meistens zumindest), eine gute Kontrolle über die eigene Architektur, und der Umstand, dass er das Recht auf seiner Seite hat. Insgesamt besteht aber grundlegend ein starkes Ungleichgewicht zwischen Angreifer und Verteidiger zugunsten des Angreifers.

Auch dies ist informationsethisch relevant, denn der Strafverfolger hat prinzipiell größere Schwierigkeiten mit dieser Form des Angreifers, während der Strafverfolger bei vielen normalen Verbrechen stark im Vorteil ist. Eine so starke Benachteiligung führt in der Folge oft dazu, dass der Strafverfolger zu besonders drastischen Mitteln greift, um eine höhere Effizienz zu erreichen.

4.7.2 Strukturmerkmal Digitale Spuren

Ebenfalls strukturell problematisch ist die Sicherung digitaler Spuren an Tatorten. Damit ist die Sicherung von Spuren auf Datenträgern gemeint. Sie muss vor allem bei Hausdurchsuchungen, aber auch bei „Online-Durchsuchungen“ stattfinden, um illegale Inhalte oder Indizien für Straftaten festzuhalten. Dies trifft auf eine eigene Menge von Schwierigkeiten, da die Kriminellen sich ihrer Kriminalität in der Regel bewusst sind und da sie entsprechende Gegenmaßnahmen ergreifen können. Eine der am weitesten verbreiteten Gegenmaßnahmen ist die Verschlüsselung von Datenverbindungen, einzelnen Daten oder gleich von ganzen Rechnern. Werden diese Verschlüsselungen vernünftig umgesetzt, ist es Strafverfolgern deutlich erschwert und oft unmöglich gemacht, die digitalen Beweise zu sichten und zu sichern. In der Praxis wird daher auch hier versucht, die Rahmenbedingungen zu ändern. Ein im Brechen von Kryptographie gängiges Verfahren stellt dabei das Abfangen von Nachrichten vor oder nach der Verschlüsselung dar, was in diesem Fall durch eine Installation eines „Trojaners“, also einer Überwachungssoftware, auf dem Rechner des potentiellen Straftäters erreicht werden könnte. Dies ist allerdings unzuverlässig und erneut problematisch im Kontext gesellschaftlicher Grundrechte, was wir unten ebenfalls noch genauer diskutieren wollen. Zusammenfassend können wir also folgende Schwierigkeiten der Spurensicherung festhalten:

- Bei einer Identifikation von Angreifern über Netzwerke stehen den Angreifern zahlreiche Möglichkeiten der Tarnung und Täuschung zur Verfügung. Datenspuren sind in diesen Kontexten sehr flüchtig und sehr formbar;

- Bei einer Sicherung von Datenspuren an digitalen Tatorten können diese Spuren zudem verschlüsselt werden, was die Einführung von Mechanismen zur Brechung oder Umgehung dieser Verschlüsselungen erforderlich macht.

Als besonders gefährliche Variante des Tarnens und Täuschens muss das gezielte Fälschen von digitalen Spuren erwähnt werden. Analysten denken oft, sie könnten aus einigen technischen Kriterien wie etwa Metadaten oder Programmierstilen Informationen über den Ursprungsort deduzieren. Das ist allerdings ein fataler Trugschluss. Denn natürlich weiß jeder Angreifer, wie Forensiker arbeiten. Der Angreifer wird also, wenn er seinen Angriff tarnen will, mit der Brille des Analysten seinen eigenen Angriff ansehen und genau untersuchen, welche Teile er in welcher Art und Weise fingieren kann, um falsche Fährten zu legen. Anders gesagt: Code lügt. Alles was an Code spezifisch sein kann, kann vom Angreifer frei erfunden und konzipiert worden sein. Ein Analyst darf sich nie sicher sein, dass eine bestimmte Menge von Eigenschaften in einem Stück analysierten Code tatsächlich

auf einen bestimmten Urheber hinweist, selbst dann nicht, wenn diese Information sehr spezifisch zu sein scheint.

B

Beispiel 4.1: Imitation eines Angreifers

Ein schlauer Angreifer könnte einen Angriff so aussehen lassen wollen, als käme er aus dem Iran. Was müsste er dazu tun? Zum einen müsste er sich ansehen, von welchen Strukturen aus ein iranischer Angreifer arbeiten würde und diese Strukturen nachbilden. Zweitens müsste er iranische Programmierstile imitieren, indem er sich etwa Code von iranischen Hackerforen besorgt. Drittens schließlich könnte er sich darum bemühen, in geheime Hackerprojekte des Irans einzubrechen, um von dort aus Code zu stehlen, den er in seinen eigenen Angriff einbauen kann. Wenn er auf diese Weise erst einmal einen „iranischen Angriff“ gebaut hat, würde er noch versuchen, die eigenen iranischen Spuren ein wenig schlecht zu vertuschen, damit ein Analyst denkt, die Iraner hätten versucht, ihre Urheberschaft zu verschleiern. Und dann wäre dieser auch schon fertig. Ein Angriff wäre das Resultat, der zu 80 % so aussieht, als käme er aus dem Iran. Da wir nun aus dem vorangegangenen Abschnitt wissen, dass Attribution auch mit politischen Willen zusammenhängt, könnte ein vermeintlicher Angriff aus dem Iran in einer gespannten Atmosphäre zwischen diesem Land und einem anderen bereits ausreichend sein, um eine politische Reaktion zu provozieren, eventuell sogar eine militärische Reaktion. Daher muss man also von allen technischen Informationen dringend Abstand nehmen. Man muss sie sicherlich beachten und kann sie als Indiz nehmen, allerdings muss man dabei gewahr sein, dass man es unter Umständen mit einem sehr raffinierten Angreifer zu tun hat, der einen auf die eine oder sogar auf diverse falsche Fährte locken will.

Diese Bedingungen für die Sicherung digitaler Spuren im Internet sind alles andere als trivial oder einfach. Daher sind die Strafverfolger auch seit einigen Jahren bemüht, einige dieser Bedingungen zu ihrem Vorteil zu modifizieren und Spuren entweder frühzeitig und unbemerkt zu sichern oder sie präventiv zu persistieren. Eine der Maßnahmen in diesem Kontext ist die sogenannte „Vorratsdatenspeicherung“, die wir etwas später noch genauer besprechen werden, da sie verschiedene Implikationen hat. So entstehen also als Folge aus diesen strukturellen Bedingungen ethische Probleme.

K

Kontrollaufgabe 4.3: Digitale Spuren

Was zeichnet digitale Spuren aus? Was gibt es für Probleme bei der Spurensicherung?

4.8 Struktur und Werte der Privatheit

Kommen wir nun zu einem Kernthema vieler gesellschaftlicher Debatten um Cybercrime: der Privatheit. Privatheit ist die Abwesenheit von Staat und Öffentlichkeit aus bestimmten Kontexten, die dem Individuum zur freien Ausgestaltung überlassen sind. Die Literatur kennt als Typen etwa die dezisionale Privatheit als die Privatheit der Entscheidung, die personale Privatheit als die Privatheit der Person oder die lokale Privatheit als die Privatheit eines Ortes. All diese Privatheiten sind keine Pauschalwerte, sondern kennen eine Reihe von Einschränkungen. Die Privatheit der eigenen vier Wände etwa ist in dem Moment eingeschränkt, in dem ein Verbrechen in diesem Raum vorliegt. Dann kann und muss das öffentliche Interesse einschreiten und durch seine legitimen Vertreter den privaten Raum, die private Entscheidung oder die private Person als solche aufheben.

Im analogen, physischen Leben sind die Grenzen der Privatheit recht festgesetzt. Auch hier gibt es immer wieder gesellschaftliche Neuverhandlungen über die Jahrhunderte. Andere und neue Kulturen empfinden andere Dinge als „privat“ als ihre Vorgänger, sodass Privatheiten keine absoluten, sondern relative Grenzen vorgeben.

Diese Relativität macht sich in digitalen Medien nun zweifach bemerkbar.

4.8.1 Neue Privatheit?

Zum einen scheinen die Informationsgesellschaften ein anderes Empfinden für Privatheit zu entwickeln. Dies äußert sich vor allem in der massiven Offenlegung der privaten Persönlichkeit in sozialen Diensten, dem Social Web. Dieses Argument kann allerdings nicht uneingeschränkt stehengelassen werden.

Drei Gründe lassen sich dagegen anführen:

(1) Obwohl es zunächst so scheinen mag, als hätte hier eine massive Erosion der Privatheit stattgefunden, finden die meisten Expositionen

der Persönlichkeit nicht in völliger Offenheit, sondern in einem selbstgestalteten Maße statt, das oft auch erfundene oder frei interpretierte Elemente enthält. Dies hängt direkt mit einer der Hauptfunktionen dieser Dienste zusammen: dem Flirten. Man präsentiert sich innerhalb dieser Dienste eher als dass man tatsächlich seine reale Person vollständig entbirgt und zur Diskussion stellt. Die reale Person ist also gar nicht betroffen, eher eine fiktive.

(2) Hinzu kommt, dass die Exposition dieser Persönlichkeit in einem in der Regel als abgeschlossen empfundenen Raum stattfindet, der von einer zwar großen und oft physisch nicht bekannten Schar Freunde ausgefüllt wird, die aber dennoch einen abgeschlossenen Personenkreis mit klaren Auswahlkriterien bilden. Die Exposition findet also nicht in der Öffentlichkeit statt, sondern in einem privaten Raum. Dass dieser Raum allerdings zum Teil dennoch öffentlich ist, indem etwa die Internetkonzerne die persönlichen Daten auswerten, kann als Kritikpunkt gegen eine vermeintliche Naivität der Nutzer angebracht werden, obwohl dieser Umstand den Nutzern aber entgegen einiger landläufiger Argumente aber durchaus bewusst ist.

(3) Schließlich kommt noch hinzu, dass die Notwendigkeit des Privaten nach möglichen Konsequenzen beurteilt wird, die in diesem Fall in den meisten freiheitlichen Gesellschaften wenig spürbar und nicht gefährlich sind, von einem bewussten Missbrauch durch Mobbing einmal abgesehen.

Die Argumente eines fundamentalen und durchgreifenden Wandels müssen also nicht vorbehaltlos akzeptiert werden, auch wenn Privatheit durchaus erneut in Aushandlung begriffen ist. Bevor wir aber diese neuen Verhaltensweisen als sanktioniert behandeln, müssen wir noch einen ethisch stärker informierten Blick darauf werfen. Denn nur, weil viele Menschen etwas akzeptieren, muss es noch lange nicht akzeptabel sein. Dies ist eine Unterscheidung aus der Technikethik, die uns an dieser Stelle anleitet, vorhandene Urteile zu Technik nicht zu schnell anzunehmen. Sie unterscheidet zwischen Akzeptanz und Akzeptabilität. Akzeptanz ist eben das, was die Menschen zu einem gegebenen Zeitpunkt als technische Realität annehmen. Die Techniksoziologie etwa vermisst diese Akzeptanzen oft mithilfe von Fragebögen und anderen Mitteln. Das Problem ist nun aber leider, dass Entscheidungen nicht automatisch damit richtig sind, dass viele Menschen sie treffen. Besonders im Kontext komplexer Technologien können sich Men-

schen hier nämlich leicht irren, wenn sie die mittel- und langfristigen oder die höherstufigen Folgen und Risiken beurteilen sollen. Zudem können sich Menschen auch in ihren ethischen Urteilen irren, wenn nicht alle Fakten bekannt sind.

4.8.2 Neue Kontexte?

Zum anderen sind die Grenzen, die Akteure und die causae der Privatheit in digitalen Kontexten zum Teil verschoben.

(1) Die Auflösung der Grenzen kommt durch die Offenheit digitaler Räume zustande, bei denen normale physische Möglichkeiten der Abgrenzung und des Rückzugs nicht mehr in herkömmlichem Maße gegeben sind.

(2) Die Neuartigkeit der Akteure kommt zustande, indem Besitzer und Rezipienten von oder Eindringlinge in Privatheit zum einen digitale personae annehmen können, die anderen Handlungsbedingungen unterliegen als die realen physischen Personen, zum anderen, da viele Teilhandlungen automatisiert stattfinden können, sodass der Computer in diesen Teilbereichen zum Handelnden wird, womit die Eindeutigkeit des Adressaten gestört wird.

(3) Die causae, also die Begründungen von Privatheit geraten in digitalen Welten ebenfalls ins Wanken, indem hier klassische Bewertungen auf neue Rahmenbedingungen treffen.

Wir werden diese Punkte nun näher und in konkreten Bezügen besprechen.

4.8.3 Privatheit und Strafverfolgung

Wir haben oben bereits bemerken müssen, dass die Effizienz der Strafverfolgung verhältnismäßig schlecht ist. Kann dies aber als Argument zu einer massiveren Einschränkung von Privatheit durch stärkere Überwachung herhalten? Wir werden hier kein juristische Besprechung dieser Frage liefern, sondern stärker auf die Hintergründe und die allgemeine Reflektion eingehen.

Hintergrund: Unschuldsvermutung

Ein wichtiger Hintergrund für das Verständnis der entsprechenden Einwände ist die Unschuldsvermutung. Sie gilt in allen Rechtsstaaten als ein grundlegendes Prinzip der Rechtsprechung und drückt sich etwa in dem Grundsatz „in dubio pro reo“ aus. Das Prinzip hat verschiedene Konkretisierungen. Eine dieser Konkretisierungen findet sich als Eingrenzung der polizeilichen Arbeit. Eine Person darf nur dann mit höherem Aufwand als einer einfachen Beobachtung observiert und überwacht werden, wenn ein konkreter Verdacht einer Straftat vorliegt. In digitalen Räumen ist nun jedoch ein konkreter Verdacht oft nicht nachweisbar, ohne entsprechende Spuren dafür zu konstatieren und zu konservieren, ohne also eine technisch bereits aufwändigere Überwachung einzuleiten. Wird dies jedoch vorgreifend getan, vor einem erhärteten Verdacht, so wird die Unschuldsvermutung verletzt.

Hintergrund: Panoptische Effekte und informationelle Selbstbestimmung

Ein anderes Problem sind sogenannte „panoptische Effekte“. Menschen, die unsicher sind, ob sie überwacht werden, passen ihre Entscheidungen an, wenn sie Konsequenzen fürchten. Sie reagieren auf die erwarteten Erwartungen ihrer Überwacher und ziehen Konformität dem Konflikt vor. Dieser sogenannte „Panoptikum-Effekt“ wurde erstmals von Michel Foucault in seinem Buch „Überwachen und Strafen“ vorgestellt. Verschiedene psychologische Untersuchungen konnten ihn in unterschiedlichen Varianten bestätigen. Als Hawthorne-Effekt wurde er in der Steigerung der Arbeitsgeschwindigkeit von Arbeitern unter Anwesenheit von autoritär übergeordneten Beobachtern entdeckt. Sogar Platzhaltern derartiger Beobachter wie Kameras oder Fotografien waren ausreichend, den Effekt auszulösen. In Experimenten mit moralisch schwierigen Themen brachte er als Social Desira-bility Response Set (SDRS) Menschen sogar dazu, gegenüber autoritär übergeordneten Interviewern die eigenen Wertvorstellungen zu verleugnen und den Erwartungserwartungen angepasste Werte vorzutäuschen. Weitere Experimente mit ähnlichem Ausgang ließen sich anfügen. Entscheidend ist bei dieser Gruppe von Effekten, dass sie manipulativ wirken. Die Anpassung wird kaum bewusst registriert. Bei Konfrontationen der Probanden mit den Untersuchungsergebnissen wurden die Verhaltensänderungen häufig nachhaltig geleugnet.

Das Leugnen indiziert ein moralisches Problem. Menschen lassen sich nicht

gerne manipulieren. Die Manipulation wird als böswilliger Eingriff in die Handlungsautonomie empfunden, über die Ausnutzung und – eo ipso – den Nachweis einer Schwäche der Urteilsfähigkeit. In dieser Spezifik der Wirkung bildet sie außerdem eine eigene Problemgestalt für ethische Beschäftigungen. Sie ist nämlich nicht nur selbst ein moralisches Problem. Sie greift auch die Fähigkeit des ethischen Reflektierens und damit des moralischen Handelns schlechthin an. Das Abwägen der Möglichkeiten innerhalb einer ethischen Entscheidung muss frei nach den eigenen Wertvorstellungen und Entscheidungsprinzipien verlaufen. Steht man dagegen unter äußerlichen Zwängen, ist die Wahl der entscheidenden Werte bereits abgeschlossen. Der Verursacher der Zwänge hat sie vorgenommen. Dem unter Zwang agierenden Entscheider bleibt nur noch ihre Interpretation auf die Umstände.

In Demokratien steigert sich dieses ethische Problem in eine gesellschaftliche Dimension. Demokratische Gesellschaftsordnungen werden nach Werthierarchien gebildet, die in gemeinschaftlicher Abwägung der individuell für relevant empfundenen Werte beschlossen werden. Die Fähigkeit individuellen ethischen Reflektierens – die Abwesenheit äußerlicher Zwänge eine condicio sine qua non – ist also tragender Gründungspfeiler der Demokratie. Wird er durch Manipulationen der Urteilsfähigkeit, also der Handlungsautonomie ausgehöhlt, verkommt die Demokratie zur Oligarchie der Manipulatoren.

Neuere, hochtechnische Mittel zur Überwachung müssen diesen Zusammenhang besonders berücksichtigen. Technische Überwachung kann panoptische Effekte auslösen. Die Überwachungsforschung hat zwar spezifische notwendige Bedingungen dafür festgehalten. Überwachung muss sichtbar sein, es muss bekannt sein, dass sich real beobachtende Menschen dahinter befinden und es müssen gravierende Konsequenzen zu befürchten sein. Sind diese allerdings in der Wahrnehmung der Überwachten präsent, wirkt jede technische Überwachung unmittelbar manipulativ. Sie ändert die Erwartungs-erwartungen, passt Wertehorizonte und Verhaltensweisen an. Und als Technik kann sie dies auf besonders großflächige Art und Weise. Durch sie wird Manipulation zur persistenten Möglichkeit. Moralität und Demokratie können in ihren tragenden Pfeilern durch eine technokratische Oligarchie von Überwachern bedroht werden.

Eine Gefahr, auf die auch der Gesetzgeber aufmerksam geworden ist. Im technisch noch kleinen Problemhorizont wurde bereits im Kontext der im

April 1983 verhinderten Volkszählung die Schädlichkeit der Überwachung und die ihrer zeitgedehnten Variante „des Sammelns von Informationen für das Wesen der Demokratie“ erkannt. Im Dezember 1983 wurde die informationelle Selbstbestimmung als Maßnahme gegen technisch induzierten Panoptismus eingeführt. Die zentrale Stelle des Urteils (C II 1 a) lautet:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...]. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

Informationelle Selbstbestimmung sichert also dem Menschen ein sicheres Wissen über ihn betreffende Überwachung und folgende Eingriffsmöglichkeiten zu. Urteilsfähigkeit und Handlungsautonomie werden wiederhergestellt. In einer ethischen Entscheidungssituation können durch technische Überwachung auftretende und potentiell zwangsförmig wirkende Effekte präventiv verhindert oder zumindest bemerkt, zusätzlich reflektiert und nötigenfalls abgestellt werden.

Totalitarismus

Einen weiteren wichtigen Hintergrund müssen wir in der Gefahr des Totalitarismus, der Bildung von Polizeistaaten sehen. Insbesondere die deutsche Vergangenheit hat gelehrt, dass hocheffiziente Überwachung hier ein gewaltiges Problem darstellen kann, was auch die spezifisch deutsche, sehr vorsichtige Haltung im Datenschutz historisch erklärt. Dabei ist zu berücksichtigen, dass Überwachungstechnik totalitäre Regierungen zwar nicht

notwendig hervorbringt – dies ist ein falsches, technik-deterministisches Argument – sie aber doch erheblich stabilisieren kann. Überwachungstechnologien, insbesondere im Internet, macht es totalitären Regierungen erheblich einfacher, Oppositionelle zu erkennen und zu verhaften. So können also Werkzeuge der Strafverfolgung auch eine sehr dunkle und gefährliche, undemokratische Seite ausbilden, die bei der Entwicklung dieser Werkzeuge, insbesondere bei der Entwicklung eines Marktes für diese Werkzeuge, dringend mitbedacht werden muss.

Persistierung von Datenspuren: Vorratsdatenspeicherung

Kommen wir damit zur Besprechung einer konkreten Maßnahme, die nun aus verschiedenen Seiten transparenter wird: der Vorratsdatenspeicherung. Die Vorratsdatenspeicherung bezeichnet das Speichern sogenannter Verkehrsdaten des gesamten Internet Traffics eines zu umreißenden Raumes über einen bestimmten Zeitraum. Uns ist nun klar, warum diese Maßnahme prima facie Sinn macht: So können die Strafverfolger der Flüchtigkeit der physischen Spuren begegnen. Sie persistieren mit der Vorratsdatenspeicherung zumindest einen Teil der Datenspuren. Die Persistierung ist allerdings begrenzt auf einen engen Ausschnitt und in ihrer Effizienz bereits recht umstritten.

Die Gegenseite wird auch unmittelbar klar. Die Vorratsdatenspeicherung verstößt zum Teil gegen die Unschuldsvermutung, indem sie konzeptionell von der potentiellen Schuld aller Netzteilnehmer ausgeht. Sie ermöglicht eine Beobachtung des Einzelnen, sodass panoptische Effekte ausgelöst werden können, die legitime Freiheiten einschränken können. Nur in dem letzten Punkt einer materiellen Nutzbarkeit zu totalitären Zwecken ist sie weniger kritisch. Dies tut sie zwar auch, sie stellt allerdings keine eigenen Strukturen dafür her, da es sich bei ihr weniger um eine Innovation und mehr um eine Organisation handelt.

In diesem Fall können wir außerdem auch klar und eindeutig ein Problem des Adressaten erkennen. Der absolute Großteil der im Rahmen einer anlasslosen Massenspeicherung erhobenen Daten wird niemals von einem Menschen, einem realen Strafverfolger auch nur gesehen. Dies eröffnet neue ontologische Optionen der Bezugnahme. Die Massenspeicherung kann als rein technischer Akt gesehen werden, sie kann als Verstetigung physischer Spuren als Naturakt konstruiert werden (nämlich der Herstellung andernfalls natürlicher Spuren) oder eben als menschliche Handlung eines juristisch adressierbaren und kriminalistisch unmittelbar handlungsfähigen

Strafverfolgers. Aufgrund der Unschärfe der Ontologien der Technik ist jede dieser Bezugnahmen korrekt, was zur Folge hat, dass „unaufgeregte“ Haltungen zu einem rein technischen Akt genauso legitim sind wie „aufgeregte“ Haltungen zu einem menschlichen Akt. Für die analytische und juristische Bewertung korrekt und nutzbar ist mithin nur die gleichzeitige Berücksichtigung aller drei Bezugnahmen (die rechtliche Diskussion überlassen wir allerdings den Juristen, die eigene Studienmodule hierzu anbieten).

Umgehung von Verschlüsselung: Bundestrojaner

Ähnlich schwierig wird das Einschleusen von Trojanern auf Rechner potentieller Krimineller beurteilt. In diesem Fall ist es allerdings so, dass bereits ein gezielter Verdacht vorliegen muss, dass die Unschuldsvermutung also nicht betroffen ist. Vielmehr wird in diesem Fall diskutiert, wie sich die Überwachung auch privater Inhalte regulieren lässt und wie die Sicherheit des eingesetzten Trojaners gewährleistet werden kann.

Kontrollaufgabe 4.4: Privatheit

Welches sind die Hintergründe unserer Sorgen um die Privatheit? In welchen Diskussionen ist Privatheit besonders wichtig?

K

4.9 Zensur

Eine weitere Maßnahme der Strafverfolgung, respektive der Strafverhinderung, ist das Blockieren von Webseiten und sozialen Diensten im Internet. Dies wird allerdings oft als problematisch empfunden, da die gleichen Techniken und Technologien auch zum Austausch von Wissen und Meinen, zur politischen Kommunikation genutzt werden. Der Vorwurf der Zensur liegt nahe. Drei Kontexte können dazu adressiert werden.

4.9.1 Sperrung von Webseiten mit Kinderpornographie

Im Jahr 2009 wurde in Deutschland in einer Initiative der damaligen Ministerin Ursula von der Leyen vorgeschlagen, Webseiten mit kinderpornographischen Inhalten zu sperren, indem bei einer Adressübertragung zu diesen Seiten keine Weiterleitung auf die eigentlichen pornographischen Seiten, sondern auf ein Stoppschild erfolgen sollte. Das vorgeschlagene Verfahren sah dazu die Erstellung von Listen durch das BKA vor, die dann an die Netzbetreiber zur manuellen Sperrung gegeben werden sollten. Dieser

prima facie unkontrovers klingende Vorschlag traf allerdings auf heftigen Widerstand in der Netzgemeinde. Diese behauptete, mit der Maßnahme würde eine „Zensurinfrastruktur“ gebaut, die – man wehre den Anfängen – ein Einfallstor für spätere politische Zensur darstellen würde. Sperren seien zudem ineffizient, da kundige Kunden die technischen Adressen kennen würden und von Netzsperren nicht aufgehalten würden. Man solle entsprechende Webseiten daher eher Löschen als Sperren. Diese Argumente der Gegner der „Netzsperren“ waren allerdings nicht besonders tragfähig. Vier Punkte waren zu kritisieren:

- Es wurde keine Zensurinfrastruktur gebaut in einem Maße, dass Zensur technisch und organisatorisch mehr oder weniger möglich war als vorher. Zensur im Netz war in diesem Maße selbstredend durch die existierende, funktionsfreie Netz- und Sicherheitsarchitektur möglich. Hier gab es keine nennenswerten qualitativen Verschiebungen.
- Das Löschen von Webseiten ist strukturell nicht andersartig als das Sperren und kann ebenso zur Zensur verwendet werden.
- Das Sperren mag den kompetenten Kunden nicht abhalten, ermöglicht aber dann aber immerhin einen eindeutigen Nachweis krimineller Energie und die klare Abgrenzung von Zufallssurfern.
- Vor allem musste aber kritisiert werden, dass Kinderpornographie kein Wissen und Meinen darstellt, sondern ein Produkt, auf das insofern die Bezeichnung „Zensur“ gar nicht angewandt werden kann.

Dieser letzte Punkt ist besonders indikativ für die Missverständnisse im digitalen Raum und die Tendenzen seiner Proponenten und Utopisten zu pauschalen Verteidigungen und Fehleinschätzungen. Die Regulierung von Kinderpornographie ist selbstredend eine Regulierung eines illegalen Produktes, keine Zensur. Das Argument des „Wehret den Anfängen“ kann also weder auf die Struktur angewandt werden, da eine solche nicht geschaffen wurde, noch auf den Prozess und seine Intention. Diese Debatte war daher eine typische „Scheindebatte“, die leider dennoch in der Presse rauf und runter debattiert wurde.

4.9.2 Sperrung von Mobbing

Ein ähnliches Urteil muss auch auf das Sperren, das Kontrollieren oder das Beobachten von Mobbing in sozialen Diensten angewandt werden. Diese Maßnahmen sind noch in der Entwicklung und gegenwärtig nicht eindeutig

festzumachen. Auch hier werden aber voraussichtlich weder besondere Strukturen generiert, noch werden politische Inhalte betroffen sein, sodass auch hier vermutlich nicht von Zensur oder der Vorbereitung von Zensur zu sprechen sein wird.

4.9.3 Sperrung von menschenverachtenden Inhalten

Einen etwas realeren Fall dagegen bildet das Sperren menschenverachtender Inhalte auf politischen Seiten wie auf rechtsradikalen oder linksradikalen Webseiten. Hier findet durchaus Zensur im Wortsinne statt, allerdings in einem kulturell und historisch begründeten und mit den Menschenrechten in Einklang stehenden Rahmen. In diesem Kontext ist es allerdings zutreffender, von Zensur zu sprechen, als in den anderen geschilderten Fällen. Insbesondere aus den USA werden auch gelegentlich entsprechende Vorwürfe gegen Deutschland erhoben.

Kontrollaufgabe 4.5: Zensur

Was ist digitale Zensur? Wie beurteilen Sie bisherige Zensurdebatten?

K

4.10 Digitale Produktpiraterie

Digitale Piraterie ist gesellschaftlich stark in der Diskussion, da es sich um ein erstaunlich weit verbreitetes und selbst in der nicht kriminellen Öffentlichkeit toleriertes und genutztes Verbrechen handelt. De facto wird digitale Produktpiraterie als tolerabel und gebräuchlich empfunden, insbesondere unter Jugendlichen und netz-affinen Personen. Dieses Empfinden rührt zum einen aus der vermeintlichen Anonymität der Tätigkeiten, zum anderen aus der hohen gesellschaftlichen Akzeptanz. Zum Teil finden sich in Argumenten der Befürworter digitaler Produktpiraterie auch Argumentationsfiguren, die eine „ausgleichende Gerechtigkeit“ verfolgen und mit dem Hinweis auf die Millionenverdienste der Musik und Filmindustrie einen kleinen Diebstahl als gerechtfertigt empfinden. Dies sind allerdings oft nur vorgeschobene Gründe. Ebenfalls vorgeschoben ist das Argument, dass in der digitalen Kopie keine physischen Ressourcen Fremder verbraucht werden wie bei einem Diebstahl, sodass also niemand zu Schaden käme. Hier wird allerdings ausgeblendet, dass die Zahlungen für mediale Inhalte nur zu einem sehr kleinen Teil der Deckung der Materialkosten dienen, zu einem größeren Teil dagegen der Entlohnung der Arbeit.

Für die Medienindustrie müssen wir festhalten, dass durch die digitalen Raubkopien und deren Verbreitung durchaus Schäden anzunehmen sind. Allerdings sind diese Schäden nur äußerst schwierig zu beziffern. Eine Schätzung der Medienindustrie, die auf einem linearen Verkaufsverhältnis beruht, die also dahingehend argumentiert, dass die Verkäufe im Vergleich zur Zeit vor der weiten Verbreitung digitaler Raubkopien dramatisch zurückgegangen sind, sind zwar in den realen Zahlen korrekt, können aber nicht eindeutig auf Raubkopien zurückgeführt werden. So haben Untersuchungen etwa ergeben, dass Konsumenten egal welchen Alters eigentlich die gleichen Geldsummen für mediale Produkte ausgeben, dass sie diese allerdings auf verschiedene alte und neue Medien verteilen. So kaufen etwa Jugendliche und Netzerfinder Personen in der Regel auch relativ häufig Computerspiele, wobei das Geld für diese Einkäufe eben nicht mehr für den Kauf von Musik und Film zur Verfügung steht. Gleichzeitig lässt sich

Abb. 4.1: Die vom Netz genommene Webseite kino.to

aber nicht leugnen, dass ein signifikanter Einfluss anzunehmen ist. Die Medienindustrie meldet weltweit pro Jahr Schäden im zweistelligen Milliardenbereich und Verluste von Jobs im Bereich von einigen 100.000 bis einigen Millionen. Auch diese Zahlen lassen sich aber kaum verifizieren. So sind etwa für den Verlust von Arbeitsplätzen nicht nur die Raubkopierer zu adressieren, sondern auch die Medienindustrie selbst, die in den vergangenen Jahren immer stärker auf digitale Verbreitungsformen gesetzt hat, durch die bedeutend weniger Arbeitsplätze nötig waren, sodass viele der verlorenen Arbeitsplätze de facto Einsparungen durch neue Vertriebsmodelle sind. Höhere, direkte Verluste lassen sich allerdings vor allem bei kleinen Unternehmen und unbekannteren Bands verzeichnen.

Bezeichnend sind in diesem Bereich aber vor allem die indirekten Kollateral-

schäden. Die massenhafte Verletzung von Copyrights ist nach wie vor einer der Haupttriebfedern für die Ausweitung von technischen Überwachungsmaßnahmen im Internet im ansonsten in dieser Hinsicht zurückhaltenden politischen Westen.

4.11 Zusammenfassung

Zu Beginn des Studienbrief 4 in Abschnitt 4.3 Informationsethik und Cybercrime wurde zunächst die Problematik von Cybercrime angesprochen. Anschließend wurde in dem Abschnitt 4.5 Komplexität in der Informationsethik Bewertungsmaßstäbe vorgestellt, die für eine Einschätzung von Komplexität genutzt wird.

In dem Abschnitt 4.6 Der Wert der Sicherheit im Kontext Cybercrime wurden die Risiken von Cybercrime erwähnt und welche Art an Schäden entstehen können. Dabei wurden monetäre und nicht monetäre Risiken berücksichtigt.

In dem folgenden Abschnitt 4.7 Strukturen der Sicherheit im Kontext Cybercrime wurden die Strukturmerkmale Identität, Internationalität, relative Effizienz und digitale Spuren näher beleuchtet und aus der Sicht des Angreifers aufgearbeitet. So wurde dargelegt, wie Angreifer diese Merkmale für ihre Zwecke verwenden.

Der Abschnitt 4.8 Struktur und Werte der Privatheit wurde die Veränderung der Privatheit durch neue Technologien genauer beleuchtet. Im Anschluss wurde in 4.9 Zensur ein Überblick über die Zensur durch Strafverfolgungsbehörden gegeben und welche Problematik damit einhergeht.

Der Studienbrief schließt mit dem Abschnitt 4.10 Digitale Produktpiraterie ab. An dieser Stelle wurde die Problematik der gesellschaftlichen Toleranz in Bezug auf Copyright diskutiert. Zusammenfassend müssen wir also feststellen, dass der Strafverfolger in diesem Bereich unter verschiedenen und je ungünstigen Bedingungen operiert.

4.12 Übungen

Ü

Übung 4.1: Meldung von Angriffen

Diskutieren Sie, an wen eine Cyber-Angriffsvorfall gemeldet werden soll. Wie ist diese Meldung zu behandeln?

Ü

Übung 4.2: Art der Schäden

Erläutern Sie, welche Arten von Schäden durch einen Cyber-Angriff entstehen können.

Ü

Übung 4.3: Vorkehrungen

Erläutern Sie, in welchem Umfang Vorkehrungen gegen Cyber-Angriffe ergriffen werden sollen.

Ü

Übung 4.4: Angreifer

Diskutieren Sie, warum die Verteidiger von Systemen vor einer höheren Herausforderung stehen als die Angreifer.

Ü

Übung 4.5: Zensur

Erläutern Sie die Probleme einer Zensurinfrastruktur.

Liste der Lösungen zu den Kontrollaufgaben

Lösung zu Kontrollaufgabe 1.1 auf Seite 14

1. ethischer
2. moralischer

Lösung zu Kontrollaufgabe 1.2 auf Seite 19

1. Meinungsfreiheit
2. Pressefreiheit

Lösung zu Kontrollaufgabe 1.3 auf Seite 23

Punkte 37, 39, 41, 42.

Lösung zu Kontrollaufgabe 1.4 auf Seite 32

(1) moralischer Subjektivismus, (2) Utilitarismus, (3) kompetenz- und situationsbezogene Ethiken, (4) Deontologie

Lösung zu Kontrollaufgabe 1.5 auf Seite 44

Herkömmliche Werte: z.B. Recht auf Information; freie Meinungsäußerung; Gleichbehandlung; Eigentum; Lohn für Arbeit; freie Verfügbarkeit von Wissen; Chancengleichheit; kulturelle Selbstbestimmung.

Neuartige Probleme: z.B. maschinelle, in Algorithmen manifestierte Selektion; digitales Kopieren; Kosten von Technik; infrastrukturelle Ungleichheit; Anonymität im Internet

Lösung zu Kontrollaufgabe 2.1 auf Seite 54

In einer Gesellschaft/Gruppe sorgen alle gemeinsam für die Sicherheit. Es ist aber auch üblich, dass nur eine bestimmter Teil der Gesellschaft für die Sicherheit garantiert und andere Personen andere Aufgaben übernehmen.

Lösung zu Kontrollaufgabe 2.2 auf Seite 55

Sicherheit ist die Abwesenheit von Gefahren oder Bedrohungen durch andere. Jede Gesellschaft definiert eigene Ziele ihrer Sicherheit, da sie selber für sich entscheiden was als schützenswert ist. Dies führt zu zwangsläufig zu unterschiedlichen Definitionen des Begriffs Sicherheit.

Lösung zu Kontrollaufgabe 2.3 auf Seite 57

Der Wert der Sicherheit ist für jede Gesellschaft/Kultur anders. Grundsätzlich hat jeder Mensch das Bedürfnis zu leben und stuft jede Bedrohung dieses Ziel als hohe Gefahr ein. Jedoch können auch Werte einer Gesellschaft über der Angst vor dem Tod stehen. Einige werten die Ziele Freiheit und Gerechtigkeit höher als ihr eigenes Leben ein.

Lösung zu Kontrollaufgabe 2.4 auf Seite 58

Wertrationalitäten sind die Vorstellungen von relativen Kausalitäten und Relevanzen auf verschiedenen Ebenen. Wobei durch die relativen Kausalitäten eine Sortierung von Ursache und Wirkung Zusammenhängen durchgeführt wird. Je nach Gesellschaftszugehörigkeit werden Kausalitäten anders wahrgenommen und rufen bei einigen Menschen Empörung hervor wohingegen andere dies bereits absehen konnten und gelassen bzw. nüchtern betrachten.

Lösung zu Kontrollaufgabe 2.5 auf Seite 62

Schutz, Dominaz, Verantwortung und Verantwortlichkeit. Das Prinzip des Schutzes bildet den Kern der Sicherheit, den es zu erreichen oder zu erhalten gilt. Die Dominanz ist ein Mittel, um dieses Schutzprinzip zu erreichen. Die Verantwortung trägt der Handlungsausführende. Wie z.B. der Soldat im Krieg oder der Polizist im Inneren. Wohingegen die Verantwortlichkeit die Pflicht des Handlungszuständigen auf seine Aufgabe ausdrückt und er für seine Handlungen rechenschaftspflichtig ist.

Lösung zu Kontrollaufgabe 2.6 auf Seite 66

Sicherheit schränkt Freiheit immer ein. Wobei mit Freiheit die Handlungsfreiheit gemeint ist. Damit wie im Naturzustand nicht das Recht des Stärkeren gilt, müssen die Schwächeren geschützt werden. Damit jeder Teil der Gesellschaft sicher ist, muss die Handlungsfreiheit z.B. der körperlichen Ge-

walt eingeschränkt werden. So muss die Handlungsfreiheit eingeschränkt werden, um für jeden in der Gesellschaft Sicherheit zu bieten.

Freiheit und Sicherheit einer Gesellschaft kann sich aber auch auf die Freiheit anderer Gesellschaften auswirken. So kann eine Ressourcenknappheit einer Gesellschaft dazu führen, die Ressourcen einer anderen Gesellschaft zu sichern. So wird im Rahmen der Selbstverteidigung die Freiheit der anderen ignoriert. Die eigene Freiheit und vor allem Sicherheit wird über die der anderen gestellt.

Lösung zu Kontrollaufgabe 3.1 auf Seite 87

Gedanken, Gefühle, Emotionen, ausgedrückte Gedanken auf Papier oder als Kunst, die nicht für die Öffentlichkeit bestimmt sind werden als private Werte bezeichnet. Insbesondere in einer Demokratie haben Bürger das Recht auf private Kommunikation. So dürfen Ermittler nicht ohne weiteres Telefonate abhören bzw. den Briefverkehr mitlesen. Dabei muss immer auf die zeitgemäße Interpretation geachtet werden. Sodass heutige Technologien für die private Kommunikation genutzt werden (z.B. Instant Messaging, Chat-Apps), die ebenfalls von der Privatsphäre eingeschlossen werden müssen.

Lösung zu Kontrollaufgabe 3.2 auf Seite 91

Die Möglichkeit der Auskunft und Steuerung der eigenen persönlichen Daten, die andere permanent Speichern.

Lösung zu Kontrollaufgabe 3.3 auf Seite 93

Die Prinzipien Verbot mit Erlaubnisvorbehalt, Datensparsamkeit und Datenvermeidung, Transparenz, Erforderliche und Verhältnismäßigkeit unterstützen bzw. bilden die Grundlage für die informationelle Selbstbestimmung. Die Prinzipien Zweckbindung und Richtigkeit und Aktualität dienen zum Schutz des Persönlichkeitsrecht, um Missbrauch der Daten zu verhindern.

Lösung zu Kontrollaufgabe 3.4 auf Seite 104

Neue Technologien entstehen schneller als der Gesetzgeber im Bezug auf den Datenschutz darauf reagiert. So entstehen Schlupflöcher, die durch Ermittlungsbehörden oder Unternehmen ausgenutzt werden können. Ins-

besondere Unternehmen nutzen Texte, die von Benutzer nicht gelesen, aber dennoch akzeptiert werden, um für sich den massenhaften Datenabfluss zu legitimieren. Das BDSG ist eine der wenigen Hürden in Deutschland, um die massenhafte Datensammlung des Verbrauchers zu regulieren. In einer Wissens-Gesellschaft sind Informationen über Verbraucher ein hohes Gut und sehr begehrt für Unternehmen. Der Datenschutz dient als Schutz vor diesen Belangen.

Lösung zu Kontrollaufgabe 4.1 auf Seite 123

Das sind die Kosten für die Bekämpfung und die Beseitigung von Cybercrime. Da diese von 10 bis 100 fache der direkten Kosten erreichen können, muss über die Angemessenheit diskutiert werden. Dabei ist zu beachten, dass Cybercrime mit wenig Einsatz hohe Schäden hervorrufen kann. (Urteile selbst!)

Lösung zu Kontrollaufgabe 4.2 auf Seite 134

Identität : Angreifer verschleiern ihre Identität

Internationalität : Nationalität, Herkunft verschleiern

Relativ Effizient : Angreifer kann hoch skalieren, sodass kleine Wahrscheinlichkeiten schon für ein Return-Of-Invest ausreichen

Lösung zu Kontrollaufgabe 4.3 auf Seite 138

Digitale Spuren sind sehr flüchtig, da diese meist nur im Arbeitsspeicher existieren. Angreifer können die Spuren aus Log-Dateien löschen. Es stellt eine Herausforderung dar, die richtige Angriffsmaschine zu finden. Angriffscode kann so manipuliert sein, dass sie von anderen zu stammen scheint.

Lösung zu Kontrollaufgabe 4.4 auf Seite 145

Durch Überwachung könnte sich die Verhaltensweise ändern, sodass Handlungen nicht mehr durchgeführt werden, weil diese irgendwann einem zu Lasten gelegt werden können. Insbesondere durch die Datenhoheit im Rahmen der informationellen Selbstbestimmung ist ein hohes Gut und soll nicht einmal durch eine Massenspeicherung von Verkehrsdaten oder einen Trojaner angreifbar sein.

Lösung zu Kontrollaufgabe 4.5 auf Seite 147

Digitale Zensur bedeutet den Zugang zu vermeintlichen schlechten Informationen zu sperren bzw. zu untersagen. Webseiten die ausschließlich zum Verbreiten von illegalen Inhalten genutzt werden, sollten gelöscht werden. Dazu gibt es eine rechtliche Handhabe. Jedoch die Zugriff zu sperren ist eine Einschränkung der Freiheit. Sperren ist technisch schwer zu realisieren. Bei einer verfügbaren Zensurinfrastruktur können Inhalte leicht ergänzt werden. So könnten Inhalte der freien Meinungsäußerung unzugänglich gemacht werden.

Verzeichnisse

I. Abbildungen

II. Beispiele

III. Definitionen

IV. Exkurse

V. Kontrollaufgaben

Literatur

[1] Anderson, Ross: Measuring the Cost of Cybercrime. (2012). http://wiki.adaptive.cs.unm.edu/readings/2012%2005%20Anderson_WEIS2012%20measuring%20cost%20of%20cybercrime.pdf

[2] Ayoob, Mohammed: The Third World Security Predicament. (1995)

[3] *Kapitel* Ethischer Kohärentismus. In: Badura, Jens: *Handbuch Ethik*. 2. aktualisierte und erweiterte Auflage. Stuttgart/Weimar : J.B. Metzler, 2011, S. 194–205

[4] Bellany, Ian: TOWARDS A THEORY OF INTERNATIONAL SECURITY. In: *Political Studies* 29 (1981), Nr. 1, S. 100–105

[5] *Kapitel* Der Utilitarismus Einleitung. In: Birnbacher, Dieter: *Texte zur Ethik*. 3. Auflage. München : dtv, 1976, S. 198–203

[6] Booth, Ken: Security an Emancipation. In: *Review of Internation Studies* 17 (October 1991), Nr. 1

[7] *Kapitel* Drei Formen des Relativimus. In: Brandt, Richard B.: *Value and Obligation*. New York : Brace & World, 1961, S. 433–440. – hier zitiert nach der Übersetzung von Herlinde Gindlhuber und Norbert Hoerster in: Dieter Birnbacher und Norbert Hoerster, Hg., Texte zur Ethik, München 1976, S. 45

[8] Capurro, Rafael: *Informationsethik. Einführung*. 2013 http://www.capurro.de/Ethik/

[9] Dewey, John: *Theory of the Moral Life*. New York : Irvington, 1996 [1908]

[10] Duden Online: *Eintrag: Moral*. http://www.duden.de/rechtschreibung/Moral#Bedeutung1a, Abruf: 16.04.2015

[11] Duden Online: *Eintrag: Recht*. http://www.duden.de/rechtschreibung/Recht#Bedeutung1a, Abruf: 16.04.2015

[12] Eisler, Rudolf: *Wörterbuch der philosophischen Begriffe*. Bd. 2. 2. völlig neu bearbeitete Auflage. Berlin : Mittler, 1904

[13] First Congress of the United States: *Amendment IV*. http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html. Version: 1789, Abruf: 29.04.2015

[14] Grimm, Dieter: *Das Andere darf anders bleiben. Wie viel Toleranz gegenüber fremder lebensart verlangt das Grundgesetz*. http://www.zeit.de/2000/08/200008.toleranz_.xml. Version: 2000, Abruf: 17.1.2013

[15] *Kapitel* Technikethik. In: Grunwald, Armin: *Handbuch Ethik*. 2. aktualisierte und erweiterte Auflage. Stuttgart/Weimar : Metzler, 2011, S. 293–287

[16] Hastedt, Heiner: *Aufklärung und Technik*. Frankfurt/M. : Suhrkamp, 1991

[17] Hobbes, T. ; Tuck, R.: *Hobbes: Leviathan: Revised Student Edition*. Cambridge University Press, 1996 (Cambridge Texts in the History of Political Thought). https://books.google.de/books?id=xE8ecw7ZaPYC. – ISBN 9780521567978

[18] Hobbes, Thomas: *Elementa philosophica de cive*. 1782 http://books.google.de/books?id=PeoTAAAAQAAJ&pg=PP28&dq=%22bellum+omnium+contra+omnes%22&redir_esc=y#v=onepage&q=%22bellum%20omnium%20contra%20omnes%22&f=false

[19] *Kapitel* Ethik und Moral. In: Hoerster, Norbert: *Texte zur Ethik*. 3. Auflage. München : dtv, 1976, S. 9–23

[20] Hough, Peter: Understanding Global Security. (2004)

[21] Illich, Ivan: *Selbstgrenzung. Eine politische Kritik der Technik*. Reinbek : Robwohlt, 1975

[22] Jonas, Hans: *Das Prinzip der Verantwortung. Versuch einer Ethik für die technologische Zivilisation*. Frankfurt/M. : Insel, 1979

[23] Kant, Immanuel: *Kants Werke. Akademie Textausgabe*. Berlin : Walter de Gruyter & Co, 1968 [1785]

[24] Karl Homann, Franza Blome-Dress: *Wirthschafts- und Unternehmensethik*. Göttingen : Vebdebhoeck & Ruprecht, 1992

[25] Kolodziej, Edward A.: Security and International Relations. (2005)

[26] Kuhlen, R.: *Informationsethik. Umgang mit Wissen und Information in elektronischen Räumen*. Konstanz : UVK Verlangsanstalt, 2004

[27] Lippmann, Walter: People, State and Fear. In: *An Agenda for International Security Studies in the Post-Cold War Era* 2 (1991)

[28] Luciani, Giacomo: The economic content of security. In: *Journal of Public Policy* 8 (1988), Nr. 2, S. 151–173

[29] Ministers, C.E.C.: *The European Code of Police Ethics: Recommendation Rec(2001)10*. Council of Europe Pub., 2002 (Legal issues). https://books.google.de/books?id=CS2uUjGRcVIC. – ISBN 9789287148315

[30] *Kapitel* Theoretische und angewandte Ethik: Paradigmen, Begründungen, Bereiche. In: Nida-Rümelin, Julian: *Angewandte Ethik*. Stuttgart : Kröner, 1996, S. 3–85

[31] Patzig, Günther: *Ethik ohne Metaphysik*. 6. überarbeitete und aktualisierte Auflage. Göttingen : Vandenhoeck & Rupert, 1971

[32] Pieper, Annemarie: *Einführung in die Ethik*. 6. überarbeitete, erweiterte Auflage. Tübingen und Basel : A Francke, 2007

[33] *Kapitel* Die Erneuerung des Rechts. In: Radbruch, Gustav: *Ethik. Lehr- und Lesebuch. Texte - Fragen - Antworten*. 3. Auflage. Stuttgart : Klett-Cotta, 2006; orig. 1947, S. 290–297

[34] *Kapitel* Aristoteles. In: Rapp, Christpof: *Handbuch Ethik*. 2. aktualisierte und erweiterte Auflage. Stuttgart/Weimar : Metzler, 2011, S. 69–81

[35] *Kapitel* Unknown. In: Rippe, Klaus P.: *Handbuch Ethik*. 2. aktualisierte und erweiterte Auflage. Stuttgart/Weimar : J.B. Metzler, 2011, S. 482

[36] Samuel Warren, Louis B.: *The Right to Privacy*. 15. Dec 1890. – 193–220 S.

[37] *Kapitel* Nachwort. In: Tenbruck, Friedrich: *Wissenschaft als Beruf*. Stuttgart : Reclam, 2006, S. 47–77

[38] Ullman, Richard H.: Redefining security. In: *International Security* 8 (1983), Nr. 1

[39] *Kapitel* Wirtschaftsethik. In: Walter Ch. Zimmerli, Michael A.: *Angewandte Ethik*. Stuttgart : Kröner, 1996, S. 290–344

[40] *Kapitel* Schwach normative und kontextualistische Ansätze. In: Werner, Micha: *Handbuch Ethik*. 2. aktualisierte und erweiterte Auflage. Stuttgart/Weimar : Metzler, 2011, S. 191–193

[41] Wolfers, Arnold: Discord and Collaboration. (1962)