

Was ist Privatsphäre?

Benedikt Müller

Betreuer: Marcel von Maltitz

Seminar Future Internet SS2018 Lehrstuhl für Netzarchitekturen und Netzdienste

Fakultät für Informatik, Technische Universität München

Email: muellben@in.tum.de

KURZFASSUNG

Während täglich immer mehr Menschen Zugang zum Internet erhalten und gleichzeitig der Wettbewerb zwischen datenverarbeitenden Unternehmen immer monopolistischer wird, ist es von zentraler Bedeutung, die Daten der Menschen zu schützen. Das wiederum kann nur funktionieren, wenn man einen sehr klaren Begriff von Privatsphäre besitzt. Diesen Begriff versucht diese Arbeit zu vermitteln, indem sie zu Beginn einen historischen philosophischen Diskurs über Privatheit und Öffentlichkeit führt. Daraufhin werden einige grundlegende Konzepte betrachtet, die sich an verschiedene Ideen aus der Natur, der Technikphilosophie, der Rechtsprechung und der Kapitalismuskritik bedienen. Außerdem wird das Konzept der kontextuellen Integrität vorgestellt, welche mehrere Sphären für die verschiedenen Bereiche des menschlichen Lebens definiert, in denen es angemessen ist, bestimmte Informationen zu teilen und andere nicht. Zuletzt geht es um Datenschutzziele, welche ähnlich wie die Schutzziele der IT-Sicherheit eine Hilfe für die Implementierung von Systemen bieten. Allerdings schützen diese, wenn sie erreicht werden, nicht nur die personenbezogenen Daten, sondern auch die Privatsphäre.

Schlüsselworte

Privatsphäre, Individualität, Öffentlichkeit, Schutzziele, Kontextuelle Integrität

1. EINLEITUNG

„Ich will nicht in einer Welt leben, in der alles, was ich sage, alles was ich mache, der Name jedes Gesprächspartners, jeder Ausdruck von Kreativität, Liebe oder Freundschaft aufgezeichnet wird“. Dies war die Antwort von Edward Snowden auf die Frage, wieso er seinem bisherigen Arbeitgeber, dem amerikanischen Geheimdienst, den Rücken zugekehrt hat und durch die Weitergabe von geheimen Dokumenten, die eine bereits vermutete globale Überwachungsstruktur bestätigt haben, eine weitreichende Diskussion über Datenschutz los getreten hat. Gleichzeitig gibt dieses Zitat aber auch einen Ausblick auf die Antwort der Frage was Privatsphäre ist, die in dieser Arbeit gegeben werden soll. Blickt man in die Vergangenheit, stellt man fest, dass man sich bereits sehr früh mit Konzepten von Privatheit und Öffentlichkeit beschäftigt hat. Jenes Konzept, dass das menschliche Leben in zwei verschiedene Sphären unterteilt, hat sich allerdings vielfach gewandelt. Wenn man es heute betrachtet, macht man dies meist aus der Sicht von Datenschutz. Einen weitreichenden Einfluss auf die Entwicklung verschiedener Auffassungen von Privatsphäre hat auch die Erfindung neu-

er Technik, wie zum Beispiel der Fotoapparat, das Telefon oder das Internet. Als am Anfang des 19. Jahrhunderts die Diskussion um ein Recht auf Privatsphäre bei einigen Juristen beginnt, sieht man das Problem noch bei den Medien, die durch Fotografien und Tonbandaufzeichnungen immer weiter in das Privatleben von Personen eindringen[17]. Heute ist das Machtverhältnis zwischen großen datenverarbeitenden Unternehmen und deren Kunden mehr in den Fokus der Datenschützer geraten. Zuletzt im Fall von Cambridge Analytica, einem Unternehmen, das ohne Erlaubnis von Facebook oder deren Nutzern Millionen von Nutzerdaten abgreifen konnte, ohne das dies bemerkt wurde.[1] Diese Gefahren ergeben sich dadurch, dass die wirtschaftliche Struktur, in der wir leben dafür sorgt, dass Unternehmen zu Monopolen tendieren[9] und auf Grund ihrer global agierenden Struktur schwieriger in Schranken zu weisen sind, was sie immer mächtiger werden lässt. Um diese Entwicklung in den Griff zu bekommen, muss der Staat und seine Behörden die Entwicklung, immer tiefer in das Privatleben einzudringen, nachahmen, was wiederum zu weiteren Grenzüberschreitungen führt und die Grundrechte der Bürger weiter verletzt. Deswegen ist der Schutz von Grundrechten ein weiterer Punkt, der in die Betrachtung von Privatsphäre einfließen muss. All diese Punkte werden nun nachfolgend betrachtet mit dem Ziel, eine genauere Vorstellung von Privatsphäre zu vermitteln, mit dem Hinblick auf die Implementierung von konkreten Systemen.

2. PRIVATHEIT UND ÖFFENTLICHKEIT

Privatheit und Öffentlichkeit lassen sich nicht so einfach definieren, vielmehr müssen beide Begriffe in ihrem historischen, philosophischen und politischen Kontext betrachtet werden. Dieser befindet sich in einem steten Wandel, wodurch sich auch unser Verständnis dieser Begriffe fortlaufend verändert. Bereits im fünften Jahrhundert vor Christus wird die Ambivalenz von Aristoteles aufgezeigt[4]. Das antike Verständnis beruht auf starken regionalen Grenzen. So wird Öffentlichkeit in der Stadt auf Plätzen und Märkten gelebt, während Privatheit alles umfasst, was zu Hause mit der Familie stattfindet. Dadurch ergibt sich auch die damalige Funktion der beiden Sphären. Während Privatheit nur dem Fortbestand der Menschheit dient, ist die Öffentlichkeit für Fortentwicklung verantwortlich. Weitere Funktionen der privaten Sphäre sind für ihn der Freiraum zur Muße und eine selbstbestimmte Lebensführung. [6] Gleichzeitig versteht Aristoteles den Menschen aber auch als Zoon Politikon, ein Wesen, welches zum einen Gemeinschaft bildet, aber zum anderen in ihr auch ein Anteil zum vollendeten Leben erhalten kann.

Habermas schreibt zu dieser Konzeption folgendes:

„Das Reich der Notwendigkeit und der Vergänglichkeit bleibt im Schatten der Privatsphäre versunken. Ihm gegenüber hebt sich die Öffentlichkeit, im Selbstverständnis der Griechen, als ein Reich der Stetigkeit und der Freiheit ab.“[4]

Man könnte auch sagen, dass die Griechen die Vernunft verstaatlicht haben. Die Kategorien, die Aristoteles geschaffen hat, änderten sich erst in der Epoche der Aufklärung wieder. Zwar teilt sich die Öffentlichkeit durch die Entstehung des Christentums in eine kirchliche und eine staatliche Sphäre, doch der Zugang zu ihnen bleibt genauso elitär, wie auch die Kategorien in denen gedacht wird.

Um zu verstehen, wie sich das Selbstverständnis der Menschen durch die Aufklärung gewandelt hat, bietet sich folgendes Zitat von Kant an, in dem er die Frage beantwortet, was Aufklärung ist.

„Aufklärung ist der Ausgang des Menschen aus seiner selbst verschuldeten Unmündigkeit. Unmündigkeit ist das Unvermögen, sich seines Verstandes ohne Leitung eines anderen zu bedienen. Selbstverschuldet ist diese Unmündigkeit, wenn die Ursache derselben nicht am Mangel des Verstandes, sondern der Entschließung und des Mutes liegt, sich seiner ohne Leitung eines anderen zu bedienen.“[8]

Kant fordert die Menschen auf, ihre Vernunft wieder selbst zu benutzen und dadurch kehrt sich das Verhältnis um.[12] Während zuvor die Kirche und der Staat die Deutungshoheit über Wahrheit, Moral und das Gute innehaben, soll nun jeder Mensch selbst über all diese Punkte entscheiden, indem man sein Verstand benutzt. Man muss hierbei aber berücksichtigen, dass sowohl das Konzept von Aristoteles, wie auch das von Kant einem Ideal entsprechen und nicht die Wirklichkeit abbilden. Dies erklärt, weshalb bereits 200 Jahre nach der Aufklärung Adorno in einem Brief an seinen Kollegen Horkheimer bereits von einer Epoche spricht, „welche die Privatsphäre zu liquidieren sich anschickt.“[2] Das größte Problem sieht Adorno darin, dass die Kontrollfunktion, die Kant der öffentlichen Meinung zuschreibt, nur legitim ist, wenn sie sich in ihrer Wahrheit ebenfalls kontrollieren lässt. Allerdings lässt sich das nur als „statistischer Durchschnittswert der Meinung aller einzelnen“[3] verwirklichen. Ein weiteres Eindringen in die Privatsphäre findet außerdem durch den Einzug von Radio und Fernsehen in der ersten Hälfte des 20. Jahrhunderts statt, die einen „Übergang vom kulturräsonierenden zum kulturkonsumierenden Publikum forcierten.“[7] Das von Kant angestrebte Ideal wird mit ihnen deutlich verfehlt. Dies liegt zum einen an ihrer Struktur, welche sich immer aus Sender und Empfänger zusammensetzt und somit keinen Widerspruch zulässt und zum anderen an ihrer Absatzorientierung, wodurch sie nur bereits bekannte Muster wieder hervorbringen.[7] Gleiches gilt auch für das Medium Internet, welches zwar bidirektional funktioniert, aber den Menschen trotzdem nicht ermöglicht sich frei zu entfalten.[12] Damit wird deutlich, wie sich die private Sphäre im Laufe der Zeit immer mehr verkleinert

hat. Hierbei wurde die in den letzten Jahren bekannt gewordene Überwachungsstruktur der Geheimdienste noch nicht in die Beurteilung miteinbezogen.

3. GRUNDLEGENDE KONZEPTE VON PRIVATSPHÄRE

Aus dem vorherigen Kapitel geht hervor, wie weit die Privatsphäre bereits eingeschränkt ist und macht damit deutlich, dass es wichtig ist, noch Bestehendes zu schützen. Allerdings lassen sich aus der Betrachtung noch keine konkreten Handlungsanweisungen ableiten, welche aber zum Beispiel unter dem Gesichtspunkt einer Privatsphäre freundlichen Implementierung von Software nötig sind. In diesem Kapitel sollen nun Konzepte betrachtet werden, welche in den späteren Kapiteln als Grundlage dienen um praktische Handlungsempfehlung zu erstellen.

3.1 Persönlicher Freiraum

Das Konzept von Privatsphäre und des persönlichen Freiraums lässt sich bis zur Tierwelt zurückverfolgen.[18] Es ist weitläufig bekannt, dass viele Tiere ein eigenes Revier besitzen, in dem sie entweder alleine leben oder es mit anderen Artgenossen teilen und es vor Eindringlingen schützen. Als Beispiel lassen sich Löwen nennen, die mit ihrem Rudel zusammen ein Gebiet besetzen, welches sie sowohl vor fremden Artgenossen, aber auch vor anderen Raubtieren verteidigen. Der Hauptgrund dafür liegt vermutlich in der Ressourcensicherung. Ein weiterer Mechanismus zum Aufteilen des territorialen Abstands zwischen Individuen wurde von E. T. Hall beobachtet[18]. Er bezeichnet den Raum, welchen Tiere zwischen einander freiwillig frei lassen, als „personal distance“[5]. Dieser lässt sich zum Beispiel bei Vögeln, die sich auf eine Stromleitung setzen, beobachten. Beim Menschen wird hierbei meist von der Intimsphäre gesprochen. Beide Konzepte finden sich beim Menschen aber auch in einem größeren Kontext wieder. Beispiel hierfür ist des Menschen eigenes Haus, das ihm einen Rückzugsort bietet und das er mit einem Schloss an der Tür vor ungebetenen Gästen schützt. Hierbei macht es allerdings keinen Unterschied, ob der Mensch in einer Villa lebt oder nur ein Zimmer als sein Zuhause ansieht. Es geht darum, dass man sich ein Umfeld schafft, in dem man gewisse Dinge erwarten kann, um nicht immer dem Unbekannten und den damit verbundenen Stress ausgesetzt zu sein. In anderen Worten, dass mit allen den Menschen zur Verfügung stehenden Sinnen nichts Neues wahrgenommen wird. In Bezug auf das eigene Haus, möchte man also nicht, dass man dort zum Beispiel ein neues Parfüm riecht, denn dies ist ein Zeichen, dass in den persönlichen Bereich eingedrungen wurde. Eine wichtige Erkenntnis zu diesem sehr grundlegenden Verständnis von Privatsphäre ist, dass dieser Raum, den man sicher erzeugt hat, nicht nur physischer Natur sein muss. Genauso lässt sich so ein Raum zum Beispiel auch im Internet schaffen, indem man bei sozialen Netzwerken einen Account anlegen kann und diesen mit vertrauten Dingen, wie Bildern und Informationen füllt. Allerdings ergibt sich dabei ein sehr großes Problem. Während man zum Schutz von physischen Räumen noch alle Sinne zur Kontrolle zur Verfügung hat, besitzt man im Internet oft überhaupt keine Möglichkeit, den dort entstandenen, privaten Raum zu schützen, sondern wird gezwungen den Schutz des privaten Raums einer anderen Partei anzuvertrauen.

3.2 Das Recht in Ruhe gelassen zu werden

Ein weiteres Konzept zum Schutz der Privatsphäre erstellen die beiden Rechtswissenschaftler S. D. Warren und L. D. Brandeis erstmals 1890[17]. Sie erkennen bereits sehr früh, welche Eingriffe die Massenmedien, zum Beispiel durch in Zeitung abgedruckte Fotografien intimer Momente, in das private Leben der Menschen ermöglichen und auch die damit verbundenen Gefahren. Als Grundlage für ihr Konzept dient ihnen das Recht auf körperliche Unversehrtheit und das Recht auf Besitz. Beides sehen sie als Grundpfeiler für menschliches Zusammenleben. Allerdings verändert sich die Interpretation im Laufe der Zeit. Während man anfangs eine reine physische Unversehrtheit gewährleistet wird, wurde später auch anerkannt, dass sowohl die Gefühle, wie auch der Verstand eines gewissen Schutzes bedürfen. Außerdem wurde akzeptiert, dass Produkte des Verstandes, wie zum Beispiel Kunst aber auch Handelsgeheimnisse, einen Besitz darstellen, den es ebenfalls zu schützen gilt. Da aber der Schutz des geistigen Eigentums, also der Schutz von konkreten Erzeugnissen geistiger Arbeit bzw. der Schutz vor Verleumdung, womit der Schutz vor falschen bzw. Rufschädigenden Behauptungen gemeint ist, nicht ausreichen um Personen vor dem Eindringen der neuen Medien in die Privatsphäre zu schützen, erstellten die beiden Juristen das Konzept, welches sie als „Recht in Ruhe gelassen zu werden“ betiteln. Darunter verstehen sie, dass jeder Mensch selbst entscheiden soll, in welchem Maß seine Gedanken, Empfindungen und Gefühle mit anderen geteilt werden sollen und wenn sie geteilt wurden, welches Maß an Aufmerksamkeit ihnen zukommen soll.[17] Dabei machen sie auch kein Unterschied, in welcher Form diese Informationen bereitgestellt werden. Das Konzept geht damit deutlich über das des Copyrights hinaus, da Copyright nur bereits sehr gefestigte Produkte des Menschen schützt. Es vermittelt, auch wenn es noch keine klaren Möglichkeiten bietet ein Recht auf Privatsphäre davon abzuleiten, bereits eine genauere Vorstellung, was es zu schützen gilt.

3.3 Recht auf Kontrollierbarkeit der eigenen Daten

Alan Westin entwickelt in seinem 1967 erschienen Buch *Privacy and Freedom*[18] das Konzept von Privatsphäre weiter. Seine Arbeit gilt als Grundlage dessen, was die meisten Menschen heutzutage unter Privatsphäre verstehen. Er unterteilt sie in vier verschiedene Kategorien, Abgeschiedenheit, Vertraulichkeit, Anonymität und Zurückgezogenheit. Mit Abgeschiedenheit ist eine physische Trennung von anderen Individuen gemeint. Unter die Kategorie der Vertraulichkeit fallen enge Freundschaften oder Beziehungen. Anonymität beschreibt das Bedürfnis des Menschen in der Öffentlichkeit unerkannt zu bleiben. Die vierte Kategorie macht sein Konzept besonders. Sie besagt, dass der Mensch bei gewissen Bereichen einen psychologischen Schutzwall zieht, der vor ungewollten Eindringen schützen soll. Diesen Wall müssen andere respektieren, wenn man gewisse Informationen nicht teilen will[18]. Als ein Beispiel für eine Überschreitung des Grenzwalls nennt er die Praktik Menschen mittels Lügendetektoren zu befragen, da durch diese Art von Befragung möglicherweise Informationen gewonnen werden, welche der Befragte nicht teilen möchte. Dieses Konzept sieht also auch einen Einschnitt in die Privatsphäre, wenn zum Beispiel Facebook Daten benutzt, die es bekommen hat, wenn Perso-

nen nicht wissen, dass wenn sie ihren Freunden Nachrichten schreiben, diese ebenfalls von Facebook gelesen werden, dies aber eigentlich nicht wollen. Man kann auch von einem Recht auf Kontrollierbarkeit der eigenen Daten sprechen. Westin betrachtet bereits den Kontext in dem Informationen geteilt werden, wie es später auch Nissenbaum macht. In seinen Kategorien wird das Umfeld, in denen sich die Informationen befinden, immer größer doch die Menge an Informationen, die preisgegeben werden, immer kleiner.

3.4 Beherrschbarkeit der Maschinerie

Die Überschrift dieses Abschnitts geht auf ein Zitat von Wilhelm Steinmüller aus dem Jahr 2009 zurück[14], in dem er den Diskurs nicht aus der bisherigen Perspektive betrachtet, in der es um den Schutz des Privaten geht, sondern, dass die Technik, so wie sie geschaffen wurde, nicht mehr kontrollierbar ist. Als anschauliches Beispiel lässt sich das E-Mail-Protokoll betrachten. Zur Zeit seiner Erfindung hatte das Internet noch eine überschaubare Anzahl an Teilnehmern. Außerdem wollte man alles möglichst einfach halten, um nicht den Überblick zu verlieren, weshalb zu Beginn noch keine Sicherheitsmechanismen berücksichtigt wurden. Dies war außerdem auch noch nicht nötig, da zumeist nur Informationen zwischen Universitäten ausgetauscht wurden, die früher oder später meist eh veröffentlicht wurden. Als aber immer mehr Menschen begannen vertrauenswürdiger Informationen auszutauschen, wurde es immer wichtiger kontrollieren zu können, was mit den über E-Mail vermittelten Daten passiert. Ein ähnlicher Verlauf lässt sich bei sehr vielen technischen Innovationen finden, welche einen Einfluss auf die Privatsphäre haben. Deswegen sollte man schon bei der Implementierung darauf achten, dass sich das System trotz zukünftiger unbeabsichtigter Anwendungen noch kontrollieren lässt.[13] Denn mit dem Verlust der Kontrolle über die Technik, verliert man gleichzeitig auch die Kontrolle über die Daten.

3.5 Machtverhältnisse

Aufgrund der Enthüllungen über die globale Überwachungs-maschinerie der Geheimdienste der USA und Großbritanniens durch Edward Snowden aber auch durch Enthüllungen über nichtstaatliche Konzerne wie Facebook, wird das Bild von „mächtigen Organisationen als Risikogeb[n]er“[15] in der Öffentlichkeit, sowohl in Deutschland, wie auch in den USA immer stärker verankert. Das Problem des Schutzes der Privatsphäre lässt sich auch aus dem Blickwinkel des Konflikts zwischen Privatperson und öffentlicher Organisation sehen. Während früher dieser Konflikt hauptsächlich zwischen Arbeiter und Unternehmen bestand, besteht er heutzutage außerdem noch zwischen Verbraucher und Unternehmen. Auf beide Konfliktsituationen lässt sich die Kritik, die Karl Marx im ersten Band des Kapitals festgehalten hat, erweitern. Dabei unterscheidet Marx zwischen Ausbeutung und Entfremdung. Der Verbraucher gibt sobald er seine Daten mit dem Unternehmen teilt meist seine gesamten Besitzrechte an ihnen ab. Dadurch wird es für ihn unmöglich, zu bestimmen was weiter mit ihnen passiert. Zum Beispiel hat man bei Facebook keinen Einfluss auf den Algorithmus, der mit den Daten, die man hochlädt, den Newsfeed generiert. Bei Marx entfremdet man sich, da man das Produkt seiner Arbeit nicht mehr wiedererkennt[10]. Im Bezug auf Datenverarbeitung findet Entfremdung statt, wenn sich man in dem Ergebnis der Verarbeitung nicht wieder erkennt. Wenn man

zum Beispiel bei seinem Newsfeed auf Facebook nicht mehr erkennt, ob die eigenen Interessen für den Inhalt des Feeds verantwortlich sind oder Entscheidungen von Facebook. Facebook gibt dabei offen zu, dass es gewisse Aufmerksamkeitsströme so lenkt, dass die Nutzer die Anwendung möglichst lange nutzen und dadurch möglichst viele persönliche Informationen preisgeben. Ein weiterer Punkt der Kritik von Marx bezieht sich auf den Ausbeutungscharakter der kapitalistischen Produktionsweise, bei welcher der Arbeiter nur einen geringen Teil des von ihm geschaffenen Wertes erhält und der Rest dem Kapitalgeber zufällt. Analog verhält es sich mit den den Betreibern von Webdiensten, welche ihre Dienste zwar kostenlos bereitstellen, was dem Lohn des Arbeiters entspricht, sie allerdings mit den Daten ihrer Nutzer deutlich mehr verdienen wie sie für den Betrieb ihrer Dienste eigentlich benötigten, was sie wiederum als Profit behalten. Gleichwohl trifft auch die Prognose von Marx, dass sich mit der Weiterentwicklung der Technik nicht die Bedingungen der Arbeiter verbessern sondern sie immer mehr ausgebeutet werden können[10], auf den Konflikt zwischen Unternehmen und Verbraucher zu. Ein Beispiel dafür ist das Smartphone, welches von Firmen wie Facebook und Google als weiteres Mittel benutzt wird um noch mehr Daten über den Benutzer zu sammeln. Sie ermöglichen ihm zwar weiterhin die kostenlose Nutzung ihrer Dienste nun auch unterwegs allerdings sammeln sie jetzt auch Daten wie den Aufenthaltsort. Der Schutz von Privatsphäre ist also auch verbunden mit marxistischer Systemkritik.

Ein weiteres Problem für eine gerechte Machtverteilung ergibt sich aus der Neigung industrieller Prozesse hin zu Standardisierung, Modularisierung, Technisierung und Automatisierung.[13] All diese Punkte bergen Gefahr für die Privatsphäre. Zum einen gibt es keinen Standardmenschen, da alle Menschen auf unbegrenzte Art und Weise unterschiedlich sind. Dies ist in einem computerisierten System aber nicht abzubilden, weshalb persönliche Daten unter Umständen in Schubladen gesteckt werden, in die sie nicht richtig hinein passen und durch die Modularisierung werden diese Zuteilungen noch weiter verschärft. Automatisierung verbindet letztlich alle genannten Punkte, deswegen ist es nötig, dass Unternehmen offenlegen, wie genau sich der Bearbeitungsprozess der personenbezogenen Daten zusammensetzt um ein möglichst gerechtes Machtverhältnis sicherzustellen. In der Praxis besteht die Sicherstellung meist aus zwei Elementen, der Datenschutzaufsicht und der verwendeten Technik. Laut Art. 37 Abs. 1 der neuen Datenschutzgrundverordnung besteht die Pflicht, einen Datenschutzbeauftragten zu benennen, wenn personenbezogene Daten von einer öffentlichen Stelle verarbeitet werden oder wenn die Kerntätigkeit des Unternehmens in der Verarbeitung solcher Daten besteht. Der Datenschutzbeauftragte ist dann für die Überwachung der Organisation verantwortlich, sodass geltende Gesetze eingehalten werden. Eine andere Möglichkeit ein gewisses Datenschutzniveau sicherzustellen, ist die erzwungene Verwendung bestimmter Absicherungstechniken. Beim Online-Banking dürfen Banken zum Beispiel die Daten ihrer Kunden nicht unverschlüsselt übertragen.

4. KONTEXTUELLE INTEGRITÄT

Mit dem konzeptionellen Gerüst der kontextuellen Integrität hat die amerikanische Professorin Helen Nissenbaum ein Diskurs geschaffen, der die Sicht auf ein Recht auf Privat-

sphäre stark beeinflusst hat. Es ist nicht an eine bestimmte Zeit oder einen bestimmten Ort gebunden,[11] sondern entsteht aus den Dichotomien, vertraulich nicht vertraulich, privat öffentlich und privat staatlich. Die zugrundeliegende Betrachtung von Nissenbaum ist, dass alles was der Mensch macht in einen gewissen Zusammenhang passiert. Sie nennt diese Zusammenhänge „Sphären des Lebens“. Das Leben jedes Menschen besteht aus vielen solchen Sphären, zum Beispiel gibt es die bereits bekannte Sphäre der Familie, die der Medizin oder die der Freunde. Diese Sphären bieten eine Plattform auf der verschiedene Normen gelten. Laut Nissenbaum lassen sich in so gut wie allen Sphären zwei Arten von Normen wiederfinden. Sie bezeichnet die beiden als Normen der Angemessenheit und des Informationsflusses.

4.1 Angemessenheit

Mit einem Beispiel lässt sich verdeutlichen was unter Angemessenheit verstanden wird. Im Kontext eines Arztbesuchs ist es angemessen mit dem behandelnden Arzt über bestimmte Krankheiten zu sprechen, während man mit dem Arbeitgeber solche Informationen in der Regel nicht teilt. Wie sehr sich die Normen in Hinsicht ihrer beschränkenden Funktion, Ausdrücklichkeit und Vollständigkeit von Sphäre zu Sphäre unterscheiden, spielt hierbei keine Rolle. Nissenbaum hält fest, dass es keine Sphäre gibt, ohne eine Norm, welche die Handhabung von Informationen regelt. Angemessenheit definiert die verschiedenen Kontexte und entscheidet, welche Informationen zu ihnen gehören.

4.2 Informationsfluss

Ein anderer Teil an Normen, ist laut Nissenbaum für den Fluss bzw. die Verteilung von Informationen verantwortlich. Als Beispiel dient ihr die Sphäre der Freunde, in der es meist sehr klar ist, welche Informationen mit anderen Freunden geteilt werden dürfen und welche geheim zu halten sind. Aus dieser Betrachtung ergeben sich verschiedene Prinzipien für die Verteilung von Informationen. So lassen sie sich entweder frei nach dem Willen der Informationsträger teilen oder müssen vertrauenswürdig, möglicherweise sogar geheim gehalten werden. Des Weiteren kann auch ein Anspruch, ein dringendes Bedürfnis oder eine Verpflichtung bestehen bestimmte Informationen zu teilen. Wenn man zum Beispiel in der Schule zu spät in den Unterricht kommt muss man den Lehrer meist über den Grund des Zuspätkommens informieren.

4.3 Probleme und Unterschiede

Ein bedeutender Unterschied zu den bisherigen Konzepten ist, dass Information nach Nissenbaum immer an ihren Kontext gebunden ist. Es gibt also keine per se öffentlichen Daten mehr, die von jeden abgegriffen werden dürfen. In Bezug auf Facebook bedeutet das, dass Daten nur für die Personen einsehbar seien sollen mit denen man sie teilen möchte und nicht für Facebooks Werbeabteilung oder die Öffentlichkeit. Es können allerdings Probleme entstehen, wenn man sich nur an bestehenden Normen orientiert. Es wird dadurch erschwert auf technische Innovationen möglichst zeitnahe zu reagieren. Außerdem besteht die Gefahr, dass ein Konzept, welches so stark an praktische Erfahrungen gebunden ist, die moralische Autorität verliert, die es benötigt, um weitläufig akzeptiert zu werden. Um diesen Problemen entgegenzuwirken schlägt Nissenbaum vor, als grundlegendes Prinzip immer den jetzigen Zustand zu bevorzugen und zu betrachten,

inwieweit dieser durch technische Neuerungen beeinflusst wird oder inwieweit bestehende Normen erweitert werden können. Zum Beispiel lassen sich die Normen, die für Briefe bestehen, ohne weiteres auf E-Mails erweitern. Jedoch sagt sie auch, dass es trotz des Status auch möglich sein soll, bestehende Normen durch neue Verfahren zu verändern. Dies soll aber passieren, nachdem man untersucht hat, in welcher Art und Weise sich die neuen Verfahren auf grundlegende Werte auswirken. Einen der sechs von Nissenbaum aufgelisteten Grundwerte bezeichnet sie als Schutz vor Schäden durch Information. Damit meint sie, dass Informationen über eine Person nicht an Andere geraten sollen, welche dieser Person schaden können. Informationen über die Adresse und den Verdienst, welche Einbrechern helfen können ihr nächstes Ziel zu bestimmen, ist ein Beispiel für solche Daten. Ein weiter Grundwert, den Nissenbaum nennt, bezieht sich auf die gerechte Behandlung von Informationen, sodass Unternehmen oder der Staat durch ihre Macht sie nicht unbegrenzt ausnutzen können. Des Weiteren sollen Menschen nicht in der Freiheit und Eigenständigkeit ihrer Handlungen beschränkt werden. Dieser Punkt geht auf die Ideale zurück, die Kant in der Epoche der Aufklärung festgehalten hat. Nissenbaum nennt unter Berücksichtigung dieses Punktes, auch das Recht auf Privatsphäre, „das Recht über die Kontrolle der eigenen Daten“ [11] Ein weiterer Punkt, welcher vor dem Eingriff neuer Techniken geschützt werden muss, ist der Erhalt von wichtigen menschlichen Beziehungen, da die Kontrolle über persönliche Informationen eine Kernbedingung ist, um Vertrauen und Intimität herzustellen. Zudem benennt Nissenbaum als Vorteil für den Staat, dass durch eine geschützte Privatsphäre, welche durch neue Verfahren nicht eingeschränkt werden sollen. Zuletzt erwähnt sie außerdem noch verschiedene Werte, die für weniger Regulierung sprechen Dazu gehören das Recht auf freie Meinungsäußerung, eine freie Presse, ökonomische Aspekte sowie eine transparente Regierung und Sicherheit. [11]

5. DATENSCHUTZZIELE

Aus den vorherigen Kapiteln wurde ersichtlich, dass Datenschutz und der Schutz der Privatsphäre sich nicht nur aus dem Bedürfnis nach Privatheit ergibt, sondern als Schutz von Individualität und Freiheit des Menschen gesehen werden kann. In Anbetracht dieser Aufgabe entwickelt Prof. Dr. Andreas Pfitzmann und Martin Rost eine Methode, die bereits bekannte Schutzziele der IT Sicherheit im Kontext des Datenschutz betrachtet, aber auch neue Schutzziele beinhaltet. Als elementare Schutzziele definieren sie Verfügbarkeit, als „gesicherter Zugriff auf Information innerhalb eine festgelegten Zeit“, Vertraulichkeit, als „Gesicherter Nichtzugriff auf Informationen“, Integrität, als „gesicherte Echtheit von Informationen“, sowie Kontingenz, als „gesichert nicht gesicherte Echtheit von Informationen“.[16] Das Schutzziel Kontingenz entsteht aus den beiden Schutzzielen Zugreifbarkeit und Nichtzugreifbarkeit, welche in einem konträren Zusammenhang stehen, welcher zu einem Problem werden kann wenn beide gleichzeitig angestrebt werden. Kontingenz soll gewährleisten, dass der Mensch gewisse Dinge erfolgreich abstreiten können, auch wenn sie ihm von „respektabler Seite“ unterstellt werden. Pfitzmann und Rost sprechen auch davon nicht durch Technik eingeengt zu werden. Von diesen vier Elementarschutzziele lassen sich einige weitere ableiten, zum Beispiel Verbindlichkeit, Verdecktheit, Anonymität oder Unbeobachtbarkeit. All diese Ziele lassen sich allerdings

nicht klar von denen der IT-Sicherheit abgrenzen. Grund dafür ist, dass Datensicherheit eine Grundbedingung für Datenschutz ist. Spezielle Datenschutzziele hingegen sind laut Pfitzmann und Rost Transparenz und Unverkettbarkeit.

5.1 Transparenz

Transparenz bedeutet, dass ein Systemteil für eine Entität beobachtbar gemacht wird. Damit ist die Transparenz eines Systems die wichtigste Voraussetzung dafür, dass ein System kontrollierbar ist. Des Weiteren unterscheiden sie noch ob es sich erkennen lässt, ob ein System nicht transparent ist.

5.2 Unverkettbarkeit

Vollständige Transparenz in Blick auf Datenschutz ist allerdings nicht ausreichend, deswegen wird das Konzept der Unverkettbarkeit eingeführt. Dieses Ziel wirkt darauf hin, dass Daten nicht miteinander verkettet werden können. Dadurch wird erreicht, dass es zum Beispiel für den Staat nur möglich ist, die Daten der Bürger für den Zweck zu benutzen für den sie erhoben wurden, auch wenn unterschiedliche Behörden verschiedene Daten möglicherweise im selben Rechenzentrum speichern. Die Aufgabe von Datenschützern ist laut Pfitzmann und Rost bestehende Verkettungen unter Bedingungen zu stellen oder aufzulösen.

5.3 Schutzmaßnahmen

Ein Vorteil der Schutzziele wie Transparenz und Unverkettbarkeit ist, dass von ihnen leicht bestimmte Maßnahmen abgeleitet werden. Um zum Beispiel das Ziel der Kontingenz bei verschlüsselten Nachrichten zu erreichen, müsste ein Verschlüsselungsalgorithmus gewählt werden, der unabhängig von der Länge der eigentlichen Nachricht stets Nachrichten mit einer gleichen Länge erzeugt.[16] Um Transparenz zu gewährleisten muss bereits bei der Konzeption eines neuen Systems eine genaue Dokumentation erfolgen. Des Weiteren muss man in der Lage sein, Vorgänge sowohl während des Betriebs mittels Monitoring, wie auch im Nachhinein durch Protokolle überwachen zu können.

6. FAZIT

Das Thema Privatsphäre ist äußerst facettenreich und verdient eine noch weitaus tiefere und umfangreichere Betrachtung, die im Rahmen dieser Arbeit allerdings nicht möglich ist. Ein Anliegen dem sie aber genüge getan hat, ist die Betonung der Bedeutung des Themas. Denn Jeder der glaubt Privatsphäre besteht, wenn er sich mit den ihn zur Verfügung stehenden Mitteln schützt, verschließt die Augen vor der Realität. Deswegen kann ich auch der häufig im universitären Umfeld anzutreffenden libertären Meinung, dass man als Konsument doch die Wahl hat sich zu schützen beziehungsweise gewisse Dienste nicht zu benutzen, aus mehreren Gründen nicht zustimmen. Zum einen ist man oft nicht in der Lage sich gewisse Dinge auszusuchen, zum Beispiel besitzt nicht jeder genug Geld um das Land in dem man lebt zu wechseln um besser durch Datenschutzgesetze geschützt zu sein. Außerdem sind die zeitlichen und monetären Ressourcen oft zu beschränkt, um sich umfangreich mit allen Eigenschaften einer technischen Innovation zu beschäftigen um dann ein Urteil zu fällen, wie weit sie die Privatsphäre beeinträchtigt und inwieweit man damit leben kann. Aber vor allem widerspricht es einem grundlegenden Prinzip der

Demokratie, dem Vertrauen. Martin Rost[14] schreibt dazu folgendes:

„Es geht um ein begründetes, begründbares, nicht blindes Systemvertrauen. Vertrauen zu gewähren und ebenso abzufordern, macht moderne Gesellschaften so besonders effektiv.“

Man könnte sogar weiter gehen und behaupten, dass es nur lohnenswert ist, ein System überhaupt zu erhalten, wenn man ihm vertrauen kann, dass es Dinge ins Positive verändert. In Bezug auf Deutschland und vielen anderen Ländern macht es Sinn, Privatsphäre zu verstärken und gefährdende Verfahren einzuschränken, damit ein möglicherweise verlorengegangenes Vertrauen der Bürger zurückgewonnen wird. Ein Zeichen des verlorengegangenen Vertrauens, nicht nur gegenüber dem Staat, sondern auch zu den Unternehmen, wie zum Beispiel Google, ist die Entwicklung, verschiedener Privatsphäre freundlicher und zum Teil dezentraler Systeme. Mit Nextcloud ist es zum Beispiel leicht möglich, einen eigenen Datenspeicher zu erstellen auf den man von Überall zugreifen kann, auch gibt es viele Messaging Apps, die die Nachrichten ihrer Benutzer Ende-zu-Ende verschlüsseln und nicht wie Facebook mitlesen. Damit sich diese Herangehensweise aber sowohl bei der Entwicklung von Systemen, wie auch bei den Anwendern weiter verankert, muss das Verständnis von Privatsphäre in allen Schichten noch erweitert werden.

7. LITERATUR

- [1] T. Adams. Facebook's week of shame: the Cambridge Analytica fallout. *The Guardian*, 2018.
- [2] T. W. Adorno. Offener Brief an Max Horkheimer. *Die Zeit*, 1965.
- [3] T. W. Adorno. *Gesammelte Schriften in 20 Bänden: Band 10: Kulturkritik und Gesellschaft. Prismen. Ohne Leitbild. Eingriffe. Stichworte*. Suhrkamp Verlag, Frankfurt am Main, 2003.
- [4] J. Habermas. *Strukturwandel der Öffentlichkeit*. Suhrkamp Verlag, Frankfurt am Main, 1962.
- [5] E. T. Hall. *The Hidden Dimension*. 1966.
- [6] B. Hans. *Privatheit – und Öffentlichkeit*, pages 35–117. Springer Fachmedien Wiesbaden, Wiesbaden, 2017.
- [7] P. Hölzing. Öffentlichkeit und Privatheit. *dis|kurs*, 8(1), 2012.
- [8] I. Kant. Beantwortung der Frage: Was ist Aufklärung? *Berlinische Monatsschrift*, 4(12):481–494, 1784.
- [9] R. Luxemburg. *Die Akkumulation des Kapitals. Ein Beitrag zur ökonomischen Erklärung des Imperialismus*. 1913.
- [10] K. Marx. *Das Kapital, Erster Band: Der Produktionsprozeß des Kapitals*. 1867.
- [11] H. Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, pages 101–139, 2004.
- [12] T. Noetzel. Am Anfang Kant, am Ende Adorno? Zum philosophisch-politischen Diskurs über Öffentlichkeit und Privatheit. *Zeitschrift für Bürgerrechte und Gesellschaftspolitik*, 37(4):39–48, 1998.
- [13] M. Rost. Zur Soziologie des Datenschutzes. *Datenschutz und Datensicherheit*, 37(2):85–91, 2013.
- [14] M. Rost. Was meint eigentlich Datenschutz? *Der Landkreis, Zeitschrift für kommunale Selbstverwaltung*, 2014.
- [15] M. Rost. Bob, es ist Bob! *FiFF-Kommunikation*, 2017.
- [16] M. Rost and A. Pfitzmann. Datenschutz-Schutzziele – revisited. *Datenschutz und Datensicherheit*, 6:353–358, 2009.
- [17] S. D. Warren and L. D. Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5):pp. 193–220, 1890.
- [18] A. F. Westin. *Privacy and Freedom*. 1967.