Privatheit im Internet

Noah Walle

23. September 2017

Zusammenfassung: Meine Ausarbeitung befasst sich mit der Privatheit im Internet. Dabei gehe ich zunächst auf den Begriff der Privatheit und seine Bedeutung für den sozialen Raum ein. Daraufhin betrachte ich den Übergang vom sozialen zum digitalen Raum und damit das Aufkommen neuer Probleme für die Privatheit, wie beispielsweise das Hinterlassen von Spuren beim Surfen im Internet. Bei den riesigen Datenmengen, die so im Internet entstehen wird auch von Big Data gesprochen. Um solche Mengen effizient verarbeiten zu können, bedarf es neuer Analysemethoden, welche ebenfalls die Privatheit einschränken können. Nach einer Auseinandersetzung mit Privatheit und Big Data gehe, ich auf den Datenschutz ein, wie dieser in Konflikt zu anderen Werten steht, welche Schutzmaßnahmen es gibt, aber auch wie Unternehmen den Datenschutz untergraben am Beispiel von Facebook. Es kommt die Frage auf, wie man Privatheit und die Privatsphäre in Zukunft gestalten kann. Dazu gehe ich auf Handlungsmöglichkeiten in Bildung, Recht, Wirtschaft und Technik ein, welche die Grundlage für eine zukünftige Privatheitskultur legen könnten. Darüber hinaus stelle ich das Konzept der Privatsphäre im Kontext vor. Dies ist ein Konzept, welches zum Ziel hat sich den Gegebenheiten des Web 2.0, also des Social Webs, anzupassen und dort für eine optimale Privatsphäre zu sorgen. Schlussendlich befasse ich mich noch mit dem Thema Freiheit versus Sicherheit. Hier gehe ich auf das Verhältnis von Freiheit und Sicherheit ein und stelle im Zuge dessen einige neue Gesetze vor, die mit der Begründung einer gefährdeten Sicherheitslage erlassen wurden und die Privatheit der Menschen im Internet stark gefährden.

Matrikelnummer: 3716854

Hiermit erkläre ich, die vorliegende wissenschaftliche Arbeit selbständig und ohne unzulässige fremde Hilfe angefertigt zu haben. Ich habe keine anderen als die angeführten Quellen und Hilfsmittel benutzt und sämtliche Textstellen, die wörtlich oder sinngemäß aus veröffentlichten oder unveröffentlichten Schriften entnommen wurden, und alle Angaben, die auf mündlichen Auskünften beruhen, als solche kenntlich gemacht. Ebenfalls sind alle von anderen Personen bereitgestellten Materialien oder erbrachten Dienstleistungen als solche gekennzeichnet.

Leipzig, den _____ _____

Ort, Datum Unterschrift

Inhaltsverzeichnis

1 Einleitung

Historisch gesehen ist die Privatheit ein junges Privileg. Erst gegen Ende des 18. Jahrhunderts und im Laufe des 19. Jahrhunderts hat die Privatheit, durch die bürgerliche Emanzipation und die Herausbildung moderner Nationalstaaten, an Bedeutung gewonnen. Der Begriff "privat" leitet sich vom lateinischen Wort "privatus" ab und bedeutet "(der Herrschaft) beraubt, gesondert, für sich stehend". Er bedeutet also eine Trennung von der öffentlichen Sphäre, vor allem vom Staat. Die Privatheit hat sich also aus dem Öffentlichen entwickelt, aber nicht in Abspaltung, sondern als Teil des Öffentlichen.

Der digitale Wandel und die Nutzung digitaler Technologien sowie deren massive Verbreitung und fortschreitenden Durchdringung sämtlicher Ebenen der Gesellschaft hat starke Auswirkungen auf die Privatsphäre der Menschen. Informationen werden öffentlich im Internet preisgegeben und liegen dort in digitaler Form vor. Damit sind diese Informationen nicht mehr flüchtig, sondern beständig und langfristig verfügbar. Außerdem sind sie mithilfe von Suchmaschinen auffindbar und lassen sich auf diese Weise zusammenführen. Auch der Vervielfältigung der Informationen steht damit nichts mehr im Weg, sie können entwendet, aus ihrem ursprünglichen Kontext gelöst werden und somit auch in ihrer Bedeutung verändert werden. Im digitalen Raum herrschen also ganz neue Bedingungen, die es erfordern, die Begriffe Privatheit, Datenschutz und Informationsschutz zu überdenken.

Mit einer angemessenen Privatheit offenbart das Internet jedoch ein ganz neues Potenzial. Es fördert die freie Entfaltung, die demokratische Partizipation und das wirtschaftliche Wohlergehen. Menschen können freie Informations- und Bildungsangebote online in Anspruch nehmen, welche ihnen bei der Entwicklung eines selbstbestimmten Lebensentwurfes helfen. Politisch engagierte Menschen können sich mit gleichgesinnten vernetzen und Interessengruppen bilden. Wirtschaftlich gesehen hat das Internet eine komplett neue Plattform für eine Vielzahl an Berufen und Unternehmen eröffnet. Seine Produkte international anzubieten war noch nie so einfach, wie es heute ist. Die Herausforderung besteht vor allem darin, eine Balance zwischen der Privatheit und dem Potenzial des Internets zu finden.

Um diese Herausforderung zu meistern bedarf es ein radikales Umdenken der Gesellschaft bezüglich der Privatheit. Aktuell ist der Umgang mit der eigenen Privatheit und Privatsphäre für viele Menschen im Internet gar kein Thema. Das verwundert allerdings nicht, denn weder in der schulischen Laufbahn, in der beruflichen Ausbildung, im Studium oder letztendlich im Beruf spielt Privatheit eine Rolle. Nutzungskompetenzen müssen von den Menschen in den meisten Fällen selber erlernt werden. Dies wird nicht gerade von der Wirtschaft unterstützt, welche sich hinter schwer zugänglichen Geschäftsbedingungen und verwirrenden Klauseln versteckt. Für die Unternehmen sind die privaten Daten ihrer Nutzer Gold wert und von selbst scheint es hier keine Änderungsbereitschaft zu geben. Seitens der Politik wird allerdings auch nicht viel unternommen, um gegen Unternehmen, wie Facebook, vorzugehen, welche ein Geschäft mit der Verletzung der Privatsphäre machen. Diese Unternehmen wissen sich in der Öffentlichkeit gut zu profilieren und erfahren so gut wie keine gesellschaftliche Ächtung, außer von Datenschützern. Auch seitens der Technik muss es hier verstärkte Anstrengungen geben um die Privatheit zu unterstützen und neue Grundlagen für einen bewussten Umgang mit ihr zu schaffen.

Während es also in Sachen Privatheit sehr viel Nachholbedarf in der Bildung, Wirtschaft und Technik gibt, wird es auch auf rechtlicher Ebene immer skurriler. So werden neue Gesetze erlassen, die die Privatheit immens verletzen. Ein prominentes Beispiel ist der Staatstrojaner, welcher nun per Gesetz auch für Alltagskriminalität eingesetzt werden kann. Ermittlungsbehörden sind seit kurzem befugt nach eigenem Ermessen den Staatstrojaner gegen Bürger einzusetzen. Das Gesetz ist so offen ausgelegt, dass hier auch unschuldige Personen infiziert werden können, wenn die Behörden es für notwendig erachten. Auch das neue Datenschutzgesetz und das Netzwerkdurchsetzungsgesetz stehen heftig in der Kritik. Ersteres stellt einen massiven Abbau des Datenschutzes da und beinhaltet, entgegen den Vorgaben der EU eigene nationale Regelungen, welche teilweise sogar gegen EU-Recht verstoßen. Letzteres Gesetz birgt laut Datenschützer eine große Gefahr für die freie Meinungsäußerung.

Die Rechtfertigung für die Gesetze bietet die aktuelle Sicherheitslage. Seit dem 11. September 2001 gab es immer wieder neue Gesetze, die die Freiheit zugunsten der Sicherheit einschränkte, weil man sich so vor dem internationalen Terrorismus schützen müsse. Diese Gesetze werden in Zeiten der Gefahr verabschiedet, bleiben dann jedoch auch in Zeiten ohne konkrete Bedrohungslage bestehen und werden nicht zurückgenommen. So entsteht ein sukzessiver Abbau der Freiheit und damit natürlich auch der Privatheit, vor allem, wenn die Gesetze der Überwachung im Internet dienen, wie beispielsweise der Staatstrojaner. Für die Privatheit und den Datenschutz ist also auch das Diskursfeld Freiheit versus Sicherheit von hoher Bedeutung in der heutigen Zeit.

Wie eingangs erwähnt ist die Privatheit nicht erst mit dem Auftreten des Internets ein wichtiges Thema. Sie spielte auch vorher eine große Rolle im gesellschaftlichen Leben und sozialen Miteinander.

Bevor ich nun zur Privatheit im Internet und dessen neue Herausforderungen komme, gehe ich zunächst auf den sozialen Raum sowie die Aufgaben und Funktionen der Privatheit in ihm ein.

2 Sozialer Raum

Das Konzept des sozialen Raums wurde vom französischen Soziologen Pierre Bourdieu entwickelt und dient der Darstellung und Analyse sozialer Strukturen und individueller Positionen. Das Konzept umfasst drei Bestandteile: Den sozialen Raum, die Klasse und den Habitus. [1]

Der soziale Raum beschreibt die objektiv erfassbaren Lebensbedingungen und die daran gebundenen beziehungsweise darin enthaltenen Wertvorstellungen, wie sie jeder Mensch für sich selbst in seinem Lebensraum seit Beginn seiner Wahrnehmung erfährt. Spezifiziert wird der soziale Raum außerdem auch durch die soziale Lage, Klasse oder das Milieu, deren besondere Umstände im Verhalten und Urteil der ihm angehörigen Individuen wiederzuerkennen ist. Der soziale Raum ist also ein prägendes Element im Heranwachsen eines Jeden und übt somit einen konditionierenden Effekt aus.

Die Klasse strebt nach Erhalt der eigenen inhärenten Identität. Sie hat eine komplexe Struktur und bezieht in ihre Identität eine Vielzahl von Faktoren ein. Existerende Klassen sind die Herrschende, die Mittlere und die Volksklasse entsprechend ihres Kapitalvolumen, kulturellen und ökonomischen Kapitals.

Der Habitus erzeugt Formen des Verhaltens und der Wertung, welche durch den Einfluss des sozialen Raums entstehen. Der Habitus eines Individuums wird durch den sozialen Raum strukturiert, welcher wiederum selbst anhand jener Strukturierungen Systeme der Erzeugung von Verhalten und Bewertungen strukturiert.

2.1 Privatheit im sozialen Raum

Die Privatheit als soziales Verhältnis drückt sich vor allem durch die Distanz beziehungsweise Nähe zu anderen Personen aus. Die Privatsphäre eines Individuums ergibt sich dabei aus seinen zwischenmenschlichen Beziehungen und deren Intensität. Sie ist vielschichtig und lässt sich neben Öffentlich in Außenbereich, Mittelbereich und Innenbereich unterscheiden. Je höher die Intensität der Beziehung, desto näher gelangt eine Person an den Innenbereich der Privatsphäre.

Der Jurist Alan F. Westin hat vier Formen der Privatheit definiert:

1. Für-sich-Sein, beschreibt die Situation des Individuums, in der es für sich allein ist und damit frei von der Wahrnehmung beziehungsweise Beobachtung durch andere.
2. Intimität, bezieht sich auf die Situation in einer Liebesbeziehung, einer kleinen Gruppe von engen Freunden oder der Familie. Hier können sich die Beteiligten im gegenseitigen Vertrauen einander öffnen.
3. Anonymität, meint die Freiheit in der Öffentlichkeit nicht identifiziert und somit nicht beobachtet oder kontrolliert zu werden.
4. Zurückhaltung, als die unterschwelligste Form von Privatheit. Sie bezieht sich auf die geistige und körperliche Zurückhaltung gegenüber anderen. Ausdruck für diese Art der Zurückhaltung sind beispielsweise Anstandsformen. [2]

Privatheit im sozialen Raum bedeutet also nicht nur einen Rückzugsort für sich und seine engen Bekanntschaften zu haben, sondern bezieht auch Anonymität mit ein. So kann man also auch, bezogen auf Handlungen und Entscheidungen, in der Öffentlichkeit privat sein, beispielsweise auf in der Kirche, auf Demonstrationen oder beim Gespräch mit Freunden im Café. Neben Räumen oder Handlungen, können auch bestimmte Informationen, wie die politische Einstellung oder der eigene Gesundheitszustand, privat sein.

Aufgabe der Privatheit ist es also, die persönliche Autonomie zu bewahren, das heißt, sie muss verhindern, dass ein Individuum von anderen manipuliert, dominiert oder bloßgestellt werden kann. Des Weiteren dient sie als emotionaler Ausgleich. Frei von sozialem Druck und gesellschaftlichen Erwartungen kann man Stress abbauen und innere Ruhe finden. Erfahrungen und Eindrücke aus dem Alltag lassen sich zur Selbstevaluation reflektieren und einordnen. Außerdem zählt auch eine geschützte Kommunikation zur Privatheit, also die Möglichkeit zu differenzieren, wem man was sagt sowie sich räumlich geschützt austauschen zu können. Die Privatsphäre ist ebenfalls ein wichtiges Konstrukt in der bürgerlichen Gesellschaft, um Folgen von Handlungen rechtlich zuordnen zu können. Damit ist die Privatsphäre ein zentraler bürgerlicher Rechtsbegriff, und damit mit der Weiterentwicklung des Rechts auch selbst weiterzuentwickeln.

2.2 Vom sozialen Raum zum digitalen Raum

Beim Übergang vom sozialen Raum zum digitalen Raum wird die Schrift nun zum Medium der Synchronizität und übernimmt damit die Funktion der Sprache. [3] Der kommunikative Austausch zwischen zwei räumlich abwesenden Personen wird mittels Tastatur und Maus möglich. Für diese Art der Kommunikation ist jedoch eine Pseudonymisierung notwendig, da die Voraussetzung für die Nutzung von Computern immer die Erstellung eines Nutzeraccounts nach sich zieht. Im Gegensatz zum Klarnamen kann man sein Pseudonym jedoch selber aussuchen. Es ist also Produkt einer selbstbestimmten Inszenierung. Das Pseudonym kann attribuiert werden und den tatsächlichen Nutzer depersonalisieren. Die mit dem Account verbundene Person kann anonym werden. Mit dem digitalen Raum findet also eine Trennung in Person und persona statt. Persona ist abgeleitet von "per-sonare" und bedeute zu deutsch "durchtönen". Ursprünglich meinte der Begriff die Maske, durch die der antike Schauspieler seine Rolle spricht, er impliziert also eine Aufspaltung in eine reale Person und eine virtuelle persona. Diese personae werden nun zu Teilnehmern einer virtuellen Gemeinschaft. Sie sind dabei aller körperlichen, geschlechtlichen, sozialen und geographischen Differenzen entkleidet und somit mit gleichen Chancen ausgestattet in ihrer Kommunikation.

Zunächst war das Internet also gekennzeichnet durch das anonyme Surfen, um die Privatheit hat man sich noch nicht so sehr gesorgt wie heute. Dies hat sich mit den sozialen Netzwerken jedoch drastisch geändert. Wo vorher Menschen mittels Pseudonymen miteinander kommuniziert haben, kommunizieren sie nun mit Klarnamen. Wo vorher keinerlei weitere Informationen zu einem Nutzer abrufbar war, ist nun ein komplettes Profil, inklusive Wohnort, Alter, Berufstätigkeit, Familienstand, Hobbies und vieles mehr sichtbar. Der soziale Raum ist somit im digitalen Raum angekommen. Und damit stellen sich auch neue Herausforderungen an die Privatheit. Die Bekanntschaften in sozialen Räumen ist deutlich limitierter verglichen mit mehreren Hundert Bekanntschaften in sozialen Netzwerken. Darüber hinaus besteht im Social Web der Zugang zu allen möglichen persönlichen Informationen, man kann eine Bekanntschaft für Jahre nicht sehen und hat dennoch die Möglichkeit über alles Bescheid zu wissen, vorausgesetzt diese Bekanntschaft veröffentlicht die Informationen. Hinzu kommt, dass die Informationen online gespeichert werden und von Dritten genutzt werden können. Was bedeutet Privatheit dann im digitalen Raum noch? Wie muss der Begriff angepasst werden?

3 Privatheit im digitalen Raum

Die digitale Privatsphäre geht aus der Anwendung des Konzepts der Privatheit auf den digitalen Raum hervor. Dabei bezieht sich die digitale Privatsphäre eher auf die äußeren Sphären. Der Mittel- oder Intimbereich der Privatheit spielt im digitalen Raum nur eine untergeordnete Rolle, wichtig ist eher die eigene Darstellung nach Außen. Die Grenzen zwischen Privatheit und Öffentlichkeit sind hier weniger sichtbar. Der Begriff der Anonymität kommt hier ins Spiel.

Die Voraussetzung für die Existenz einer digitalen Privatsphäre ist nur gegeben, wenn der Nutzer über einen Account einen Service in Anspruch nimmt. Die Zuordnung von digitaler Identität und realer Person geschieht über eine Authentifizierung. Diese erscheint als ein privater Akt, benötigt jedoch einen Authentifizierer als technische Gegenseite und beinhaltet somit einen übergeordneten rechtlichen Kontext. Durch die Verbindung der digitalen Identität mit einem Account können Handlungen, für welche die üblichen rechtlichen Konstrukte der Zurechenbarkeit von Handeln gelten, im Internet zugeordnet werden.

Ist diese Verbindung zwischen digitaler Identität und realer Person nicht gegeben, so kann die Privatsphäre als Konstrukt der bürgerlichen Rechtsordnung, um Folgen von Handeln rechtlich zuordnen zu können, nicht greifen. Die Möglichkeit privater Geschäfte jenseits der Rechtsordnung entsteht. Technisch wird es uns also ermöglicht die Zurechenbarkeit unserer Handlungen zu verschleiern und somit der rechtlichen Verantwortung zu entgehen. Aufgrund dieser Begebenheiten können im digitalen Raum, wie auch im sozialen, Schwarzmärkte entstehen. Diese sind jedoch physisch nirgendwo verortet, lediglich eine anonyme Kommunikation zwischen Käufer und Verkäufer ist von Nöten.

Die Privatheit ist ein wichtiger Aspekt sozialer Interaktion. Ein politisches Gespräch unter Freunden sollte beispielsweise nicht unbedingt von Arbeitskollegen gehört werden. Auch im Internet muss es die Möglichkeit geben die Privatheit so zu gestalten, dass man sich zeigen oder verbergen kann, je nach dem wer mein Gesprächspartner ist oder über was man sich unterhält. Menschen bewegen sich stets in unterschiedlichen Rollen beziehungsweise Kontexten (beruflich, privat, Famile, Bekanntschaften, ...) und passen dementsprechend die Freigabe ihrer persönlichen Informationen an. Wie und was man in welchen Kontexten teilt ist dabei maßgeblich von der Kultur abhängig. Die Kultur bezeichnet im groben alles das, was Menschen selbst gestaltend hervorbringen und umfasst Kunst und Technik, aber auch Recht, Werte,

Wirtschaft und Wissenschaft. Es bringt ein Gebilde aus expliziten und impliziten Regeln und Vorstellungen hervor, welche die Praktiken und Interaktionen der Menschen untereinander stabilisieren. Diese Regeln einer Kultur sollten auch technisch umsetzbar, also auf die Kommunikation im Internet, übertragbar sein. Aufgrund der Natur des Internets ist es schwer zu entscheiden welches Maß an Privatheit in welcher Situation angemessen ist. Dienste im Internet können einen Raum bieten für politische Diskussionen, Informationsquellen oder Vernetzung mit anderen Menschen. Sie tragen also heutzutage maßgeblich zur eigenen Entwicklung bei, nehmen es aber mit der Privatheit nicht immer so eng. Hier muss ein Kompromiss gefunden werden, um eine angemessene Privatheit zu garantieren.

3.1 Nutzungskompetenzen und Gestaltungsmöglichkeiten

Wichtig für eine angemessene Privatheit ist, dass die Nutzer sich der Möglichkeiten des Internets, ihre Selbstentfaltung, die Möglichkeit zur politischen Partizipation und ihren Wohlstand zu unterstützen, bewusst sind. Gleichzeitig sollten sie die Risiken kennen, welche sich aus möglichen Verletzungen ihrer Privatheit für sie ergeben können. Diese beiden Aspekte müssen sorgfältig abgewägt werden können um einen, den Präferenzen der Nutzer, entsprechenden Umgang mit der Privatheit im Internet entwickeln zu können. Gestaltungsmöglichkeiten sollten dabei für Nutzer vorhanden, verständlich und handhabbar sein. Der Privatheitsschutz sollte also nicht in den Verantwortungsbereich des Einzelnen fallen, da die hohe Komplexität des Internets und seiner Dienste sowie die Heterogenität der Nutzergruppen es für den Einzelnen unmöglich machen, alle potenziellen Einschränkungen der Privatheit und deren mögliche Konsequenzen einschätzen und entsprechend reagieren zu können. Es muss also ein Vertrauensverhältnis zwischen den Nutzern untereinander und ihren Diensten bestehen.

3.2 Vetrauenswürdigkeit im Internet

Das Internet und seine Dienste sowie Teilnehmer sollten unabhängig von den Kenntnissen, Vorlieben und Aktionen der einzelnen Nutzer einen grundlegenden Schutz der Privatheit garantieren. Hier sind vor allem die Anbieter von Dienstleistungen gefragt. Diese sollten angemessene Regeln für ihre Dienste aufstellen. Dazu kann beispielsweise Datensparsamkeit gehören, also den Dienst so gestalten, dass möglichst wenig persönliche Daten benötigt werden. Aber auch Nutzer untereinander sollten sich an gewisse Regeln und Verhaltenskodizes halten. Freunde in sozialen Netzwerken müssen auf den Schutz ihrer Privatheit untereinander Acht geben, nicht jeder möchte beispielsweise ohne Zustimmung auf Fotos oder Beiträgen markiert werden.

3.3 Häufige Einschränkungen

Angemessene Privatheit ist oft nicht garantiert, da entweder Nutzungskompetenzen und Gestaltungsmöglichkeiten der Nutzer einerseits und/oder die Vetrauenswürdigkeit der Dienste andererseits noch nicht weit genug ausgebildet sind. Aktuell ist es immer noch schwierig für Nutzer ausreichende Kenntnisse über die Nutzung persönlicher Daten durch Internetdienste zu erlangen. Oft ist auch schleierhaft, nach welchen Regeln die Dienstleister die Daten verarbeiten und weitergeben. Die Gestaltungsmöglichkeiten in Hinblick auf Privatheitspräferenzen sind ebenfalls oft eingeschränkt, viele Dienste bieten schlichtweg nicht genug Auswahlmöglichkeiten um den Nutzern gerecht zu werden. Die Einstellungen sind dabei auch nicht immer leicht verständlich und nutzbar. Darüber hinaus beziehen sie sich oft nur auf die Daten, die direkt vom Nutzer gesammelt werden und nicht auf die Informationen, die aus diesen Daten abgeleitet werden. Ob und wie die Daten an Dritte weitergegeben werden liegt in vielen Fällen auch nicht in den Händen der Nutzer. Gesetzliche Regelungen zum Schutz der Privatheit sind uneinheitlich und orientieren sich teilweise nicht an den Begebenheiten des modernen Internets. Das führt dazu, dass manche Anbieter mit persönlichen Daten anders umgehen, als es gesetzlich vorgeschrieben ist und den Nutzerpräferenzen entsprechen würde. Außerdem wird es immer schwerer den Schutz der Privatheit durchzusetzen, wenn Daten an Dritte weitergeben werden. Neben willentlich bekanntgegeben Informationen werden beim Surfen auch Spuren hinterlassen, dessen sich die Nutzer nicht immer bewusst sind.

3.4 Digitale Spuren

Genauso wie wir Spuren hinterlassen beim Wandern durch den sozialen Raum, so hinterlassen wir auch Spuren beim Surfen durch das digitale Universum. Jedoch hinterlassen wir nicht nur bei jedem Klick im Internet Spuren, sondern werden dabei gleichzeitig auch gezielt verfolgt und ausgewertet. Egal was wir machen, sei es Nachrichten lesen, auf Amazon eine neue Lampe kaufen oder sich durch die Timeline von

Facebook scrollen, wir hinterlassen wahnsinnig viele Spuren und geben diese, ob wir wollen oder nicht, an Unternehmen zur Analyse weiter.

Auf diese Weise sammelt beispielsweise Google Daten aus unseren Suchbegriffen und besuchten Websites, um personalisierte Profile mit errechnetem Alter, Geschlecht und Interessen zu erstellen. Diese Profile werden dann für personalisierte Werbeanzeigen genutzt. Auch ein auf einer beliebigen Website eingebetteter "Gefällt mir"-Button von Facebook reicht für das Unternehmen aus, um zu wissen, dass wir auf eben jener Website waren. Somit kann Facebook durch unser Surfverhalten und selber in unseren Profilen preisgegebenen Daten, Online-Profile von uns erstellen, welche die Interessen der Nutzer widerspiegeln. Diese Profile werden dann an Firmen für personalisierte Werbeanzeigen verkauft.

Die Werbeunternehmen interessieren sich jedoch nicht für die Einzelpersonen, viel mehr werden aufgrund einer großen Menge von Nutzerprofilen verschiedene Zielgruppen herausgefiltert. Somit können gleich mehreren tausend Menschen mit ähnlichen Interessen die selbe Werbung gezielt angezeigt werden. Geht es um die eindeutige Identifizierung von Nutzern interessiert das meist die Polizei oder Geheimdienste, so gibt es zahlreiche Anfragen von Ermittlern an soziale Netzwerke und E-Maildienste. Darüberhinaus zeigen die Enthüllungen von Edward Snowden, dass Geheimdienste offenbar Unternehmen auch dazu zwingen Daten herauszugeben.

Digitale Spuren in Form von selbst erstellten Profilen in sozialen Netzwerken oder auf anderen Plattformen stehen im Gegensatz zu jenen Daten, die wir beim bloßen Fortbewegen durch das Netz hinterlassen. Diese Daten werden auch Metadaten genannt. Metadaten können beispielsweise E-Mail-Adressen und -betreff, Zeit und Ort sein. Die Rückschlüsse, die man aus den Metadaten ziehen kann, sind in der Regel größer, als die der Kommunikationsinhalte selber. Darüber hinaus sind sie sehr einfach zu analysieren, da sie im Gegensatz zu Inhaltsdaten eine Struktur besitzen. Außerdem kann man nicht Surfen, ohne Metadaten zu erzeugen. Echtzeitkommunikation ohne das Hinterlassen von Verbindungsdaten ist schlichtweg nicht möglich. Durch den technologischen Fortschritt entstehen immer neuere und immer bessere Möglichkeiten große Massen an Metadaten zu rastern und zu analysieren. Je größer die Menge an Informationen und je besser sie aggregiert und analysiert werden kann, desto mehr Erkenntnisse werden aus ihr gewonnen. Dies führt uns zu dem Begriff Big Data.

4 Privatheit und Big Data

Das Social Web, auch Web 2.0 genannt, ist gekennzeichnet durch die Teilnahme mehrerer Milliarden Nutzer an den sozialen Netzwerk. Ganz vorne dabei vor allem Facebook und Twitter. Die sozialen Netzwerke ändern die Rahmenbedingungen für die Privatsphäre auf gravierende Art und Weise. Die Voraussetzung für die Teilhabe am Social Web ist die Preisgabe von persönlichen Informationen. Aufgrund der immens hohen Anzahl an Usern war die Verfügbarkeit von privaten Informationen noch nie so umfassend wie sie jetzt ist. Dazu kommt, dass die Informationen in digitaler Form vorliegen und damit langfristig verfügbar sind.

"Ich habe doch nichts zu verbergen", wird einem dann oft entgegnet, wenn man Kritik an diesem Umstand äußert. Diese Aussage ist jedoch ein Irrtum. Es kann jedem schaden, wenn bestimmte private Informationen öffentlich werden, auch wenn diese nicht rechtswidriger Natur sind, wie beispielsweise eine schwere Krankheit. Die Daten, die von einer Person gesammelt werden vermitteln kein feststehendes, objektives und immer richtiges Bild, sondern entstehen durch Verarbeitung, Verknüpfung und Verwertung vieler einzelner Informationen. Aus diesem Grund kann das Bild, das andere Personen gewinnen, ganz anders aussehen als es die betroffen Person selbst für korrekt hält.

Wie im Abschnitt Digitale Spuren bereits erwähnt, sind die Daten, die freiwillig in sozialen Medien preisgegeben werden, nur ein kleiner Teil der Datenspur. Die Datensammlung, die abseits der selbst freigegebenen Informationen stattfindet, stellt weitaus größere Probleme im Kontext des Datenschutzes dar. Das Internet wird so zum Instrument der Überwachung aufgrund der permanenten Verfolgung, Aufzeichnung und Auswertung von Metadaten und wird damit zu einer konkreten Bedrohung für die Privatsphäre.

4.1 Big Data

Big Data ist ein Sammelbegriff für die riesigen Datenmengen, die überall entstehen und mit herkömmlichen Speicherungs- und Analysewerkzeugen nicht mehr zu bewältigen sind. Um diesen Datenmengen gerecht zu werden und weil sie die Daten ohnehin schon besitzen, entwickeln große Internetkonzerne, wie Google oder Facebook neue Programme zur Auswertung und Analyse dieser Datenmengen. Sie sind getrieben von dem Interesse, die Daten kommerziell besser nutzen zu können. Dazu sollen die Programme statistische

Trends und Muster, Gesetzmäßigkeiten oder Korrelationen zwischen einzelnen Merkmalen erkennen. Diese Informationen dienen dann beispielsweise zur frühzeitigen Erkennung von Gefahren, zur Risikominimierung, zur Zeitersparnis oder auch zur Ausübung von Kontrolle und Macht. Die Auswertung personenbezogener Daten geschieht vor allem mittels Tracking und Scoring.

4.2 Tracking und Scoring

Tracking und Scoring ermöglichen eine Vorhersage über das zukünftige Verhalten eines Users. Dazu werden Profile einer Person oder Personengruppe erstellt. Diese beinhalten beispielsweise Interessen, Aufenthaltsorte, Sozialkontakte, Kreditwürdigkeit, Verhalten oder die Gesundheit der Menschen. [4]

Beim Tracking wird das Verhalten von Personen anhand bestimmter Eigenschaften verfolgt. Führt man ein Handy mit sich, so verrät es den Standort, die Bewegung, geführte Gespräche und deren Nummern sowie Zeit und Dauer der Telefonate. Der Inhalt der Kommunikationen wird dabei nicht berücksichtigt. Beim Surfen durch das Internet werden Nutzungs- und Konsumverhalten beobachtet. Beim besuchen einer Website werden so dutzende Tracking-Vorgänge ausgelöst, die meisten von ihnen gehen von großen Werbenetzwerken aus. Das Surfverhalten offenbart so Interessen, Vorlieben, Sorgen und Gedanken. Das Ziel ist es mittels automatisierter Online-Auktionssystemen personalisierte Werbung anzuzeigen. An Anonymität ist also nicht zu denken, ohne sich vor Tracking zu schützen.

Beim Scoring findet eine zahlenmäßige Bewertung von Eigenschaften einer Person durch mathematisch-statistische Analyseverfahren statt. Dabei werden Erfahrungswerte aus der Vergangenheit genutzt, um das zukünftige Verhalten einer Person vorherzusagen. Die Vorhersagen basieren dabei auf bereits vorliegende Werte vergleichbarer Merkmale anderer Personen. Es wird angenommen, dass ein ähnliches Verhalten bei der zu überprüfenden Person vorausgesagt werden kann. Diese Einschätzungen können sich auf ganz verschiedene Bereiche des menschlichen Verhalten beziehen. So kann die zukünftige Arbeitsleistung vorhergesagt werden oder die Wahrscheinlichkeit für kriminelles Verhalten ermittelt werden. Auch eine Prognose des Gesundheitszustandes oder der Kreditwürdigkeit lässt sich aufstellen.

Auf Basis der Daten findet eine Bewertung, Klassifizierung, Vermessung und Profilbildung statt. Aus diesen Profilen lassen sich religiöse und politische Einstellungen, gesundheitliche Verhältnisse, sexuelle Ausrichtung und selbst Gefühle und Stimmungen ableiten. Es ergeben sich also umfassende Möglichkeiten zur Manipulation, Diskriminierung, sozialen Kontrolle und Überwachung. Big Data hat somit das Potenzial die eigene Entscheidungs- und Handlungsfreiheit einzuschränken. Wie steht es dann um die Privatsphäre?

4.3 Privatsphäreverletzungen

Durch das Social Web entstehen neue Risiken für die Privatsphäre. Sie kann auf der Basis von eigens oder von anderen über einen selbst im Netz veröffentlichten Daten verletzt werden. Ein weiteres Risiko stellt die unkontrollierbare Verwendung von privaten Daten durch kommerzielle Datensammler dar. Folgen der Nutzung des Social Webs können beispielsweise Mobbing, Stalking, Identitätsdiebstahl, Bloßstellungen oder Beleidigungen sein. Es können auch ernste Reputationsschäden entstehen, die einem den Job kosten können oder die Chancen auf einen neuen Job minimieren. Der Schutz vor der unkontrollierten Verwendung privater Daten ist eine notwendige Voraussetzung für die Ausbildung einer Identität. Wird dies gefährdet, so wird dem Menschen das Recht auf ein selbstbestimmtes Leben genommen. Wird den Menschen das Recht genommen, selber entscheiden zu können, was über sie vergessen werden soll und was nicht, so werden sie in der Identitätsbildung behindert.

Big Data verletzt die Privatsphäre der Menschen auf unterschiedliche Art und Weise. Durch Tracking und Scoring werden Menschen klassifiziert. Der Einzelne wird also entpersonalisiert und konformisiert. Die Menschen werden so aufgrund ihrerer durch Big Data vorhergesagten Neigungen beurteilt und nicht aufgrund ihres tatsächlichen Verhaltens. Man wird eingeschränkt in der Chance sich anders zu verhalten als vorhergesagt, was Auswirkungen auf die eigene Zukunft haben kann. Man stelle sich vor, dass mittels Big Data Analysen Arbeitssuchende beurteilt werden und nun der Algorithmus anstelle des Menschen über Zusage oder Ablehnung entscheidet. Verhaltensvorhersagen durch Big Data gefährden hier auch insbesondere unsere Handlungs- und Entscheidungsfreiheit. Das Kernproblem ist also, dass aus unseren Datenspuren ein "digitales Ich" angefertigt wird, welches nicht unbedingt identisch mit der realen Person ist. Es ist jedoch genau das, was Wirtschaftsunternehmen und Sicherheitsbehörden von uns kennen. Es ist unmöglich mittels digitaler Datenerfassung moralische Einstellungen oder menschliche Handlungen zu erfassen, die eben eine Person tatsächlich ausmachen.

"Du bist das Produkt!" sollte das Motto der sozialen Netzwerke heißen. Die Nutzung ist zwar kostenfrei, bezahlt wird jedoch mit einem detaillierten Einblick in das eigene Verhalten, die eigenen Präferenzen und Interessen. Kurz gesagt, man bezahlt für die Nutzung mit der eigenen Identität. Die Äußerungen und

Handlungen, die man im Social Web tätigt, sind in den meisten Fällen privater Natur. Sie sind jedoch permanent kommerziellen Interessen unterworfen.

Eine weitere Verletzung der Privatsphäre ist die permanente Überwachung. Es findet eine umfassende Dokumentation des Online-Verhaltens statt, die wie oben beschrieben die persönliche Freiheit jedes Einzelnen einschränken kann. Die Aussage "Wer nichts zu verbergen hat, habe auch nichts zu befürchten" stellt alle Nutzer unter Generalverdacht und greift das Wesen der Freiheit an, nämlich das Recht auf Diskretion, dass man selber entscheiden kann, was man von sich preisgibt und was nicht. Darüber hinaus kann die ständige Datenerfassung Menschen dazu veranlassen, sich in ihrem Verhalten einzuschränken, um nicht aufzufallen. Dies hat fatale Folgen für die Meinungsfreiheit und Autonomie der Menschen in einer Demokratie, wenn Menschen die eigene Meinung verschweigen oder Kontakte zu Menschen mit abweichender Meinung unterbinden, nur um sich stromlinienförmig zu verhalten.

Die Technik an sich sollte hierbei nicht kritisiert werden, jedoch der Umgang mit ihr. Sie wird für eine Monopolisierung der Macht genutzt. Je mehr wir unter diesen Umständen auf Big Data vertrauen, desto mehr vetrauen wir auch auf seine Korrelationen, anstatt auf Theorie, sozial abgestimmte Erkenntnis-Interessen und für wahr befundene Gründe. Lassen wir uns durch Big Data unser Handeln diktieren, so rechnen wir unsere Handlungsfreiheit und Autonomie systematisch aus dem menschlichen Verhalten. Ersetzen wir unseren moralischen Kompass durch Vorhersagealgorithmen, so ist der Wille des Einzelnen, dem des Kollektivs schutzlos ausgesetzt.

5 Datenschutz

Datenschutz beinhaltet den Schutz des Bürgers vor Gefahren, die eine Erhebung, Verarbeitung oder Nutzung seiner Daten mit sich bringt, insbesondere die Sicherung des Grundrechts auf informationelle Selbstbestimmung. Im Vordergrund des deutschen Bundesdatenschutzgesetzes steht dabei das grundsätzliche Verbot der automatisierten Verarbeitung personenbezogener Daten. Diese Daten können also nur mit Einwilligung des Betroffenen genutzt werden.

Der Begriff Datenschutz ist Teil der Informationssicherheit. Diese beschreibt den Zustand eines Informationssystems, in dem die unberechtigte Nutzung von Ressourcen erschwert und möglichst erkannt wird. [5] Unberechtigte Nutzung heißt hier, dass ein Benutzer, dem nicht die entsprechende Rechte erteilt wurden, Daten einsehen und verändern kann oder einfach nur das System entgegen der Vorstellungen des Betreibers nutzt. Eine unberechtigte Nutzung liegt ebenfalls vor, wenn ein Nutzer mit vorhandener Berechtigung seine Aufgabe nicht entsprechend den ihm zugeteilten Aufgaben und Rechten erfüllt. Die Informationssicherheit umfasst den kompletten Bereich der Informationsarbeit und soll drei zentrale Schutziele sicherstellen:

1. Vertraulichkeit, also die Eigenschaft eines Systems, nur berechtigten Subjekten den Zugriff auf bestimmte Objekte zu gestatten und unberechtigten Subjekten den Zugriff auf alle Objekte zu verwehren.

2. Verfügbarkeit, also die Wahrscheinlichkeit, dass ein System zu einem vorgegebenen Zeitpunkt in einem funktionsfähigen Zustand anzutreffen ist.

3. Integrität, also die Eigenschaft eines Systems, die Korrektheit der Objekte sicherzustellen.

Weitere Schutzziele sind Authentisierung, Nicht-Zurückweisung, Rechtsverbindlichkeit, Anonymität, Pseudonymität, Abrechenbarkeit und Unbeobachtbarkeit.

Neben dem Datenschutz enthält der Begriff Informationssicherheit auch den Begriff Datensicherheit. Bei der Datensicherheit geht es im Gegensatz zum Datenschutz um das technische Ziel, Daten jeglicher Art ausreichend gegen Verlust, Manipulation oder andere Bedrohungen zu sichern. [6] Eine hinreichende Datensicherheit ist die Voraussetzung für effektiven Datenschutz. Sie beinhaltet Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten, der dauerhaften Sicherstellung von Vetraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste und der raschen Wiederherstellung personenbezogener Daten bei einem physischen oder technischen Zwischenfall. Darüber hinaus beinhaltet die Datensicherheit Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit dieser technischen und organisatorischen Maßnahmen.

Neben dem Begriff der Informationssicherheit, welche die Begriffe Datenschutz und Datensicherheit beinhaltet, gibt es noch den Begriff des Informationsschutzes. Dieser bezeichnet den Schutz von Informationen vor unberechtigtem Zugriff- oder Einsichtnahme, sowie die Nachvollziehbarkeit von Vorgängen in Bezug auf Informationen. [7] Er umfasst sämtliche Maßnahmen zum Schutz von Informationen vor

Verlust, Diebstahl, unbefugter Manipulation und unerwünschtem und widerrechtlichen Abfluss durch Fahrlässigkeit, Verrat oder Spionage. Die Maßnahmen betreffen den Informationsprozess, also die Erstellung, Verarbeitung, Übermittlung, Ablage und Vernichtung von Informationen. Die Informationsträger, aber auch das Zwischenmaterial oder die Informationen selbst sind vor passiven (Feuer, Wasser) und aktiven Gefahren (Spionage, Verrat) zu schützen. Dem Informationsschutz unterliegen vor allem klassifizierte und betriebsnotwendige Informationen.

5.1 Wertekonflikte

Die Privatsphäre ist eine notwendige Voraussetzung für die Ausbildung der eigenen Identität und den Schutz der individuellen Autonomie. Daher kann Freiheit nur realisiert werden unter der Bedingung einer geschützten Privatheit. Der Schutz der eignen persönlichen Daten ist gleichzeitig der Schutz meiner Privatsphäre. Dieser Selbstschutz kann jedoch mit anderen Wünschen konkurrieren und zu Wertekonflikten führen. Er kann im Widerspruch zu dem Bedürfnis stehen, sich darzustellen und auszuprobieren, nach sozialer Anerkennung und Teilhabe zu streben, immer erreichbar und informiert zu bleiben. Es gilt Kompromisse zu finden. Bin ich bereit gewisse Dienste in Anspruch zu nehmen, welche das preisgeben von privaten Informationen erfordern? Sollte ich Dienste wie sie Google und Facebook anbieten in Anspruch nehmen, obwohl diese Unternehmen schleierhaft mit meinen Daten umgehen? Sollte ich Apps herunterladen, die meine gespeicherten Daten zugreifen dürfen? Hier muss jeder für sich entscheiden, wie viel er oder sie von sich preisgeben möchte. Wichtig ist hier eine Aufklärung im Umgang mit den modernen Medien, diese ist jedoch oft nicht vorhanden.

Die grundlegenden Werte der europäischen Tradition und Gegenwart, die durch das Internet gefördert, aber auch durch die Verletzung der Privatheit gefährdet werden, sind die freie Selbstbestimmung, die demokratische Partizipation und das wirtschaftliche Wohlergehen.

5.1.1 Freie Selbstbestimmung

Die freie Selbstbestimmung bezeichnet die Möglichkeit des Einzelnen, eigene Lebensoptionen zu entwickeln und aus ihnen frei auswählen zu können, darunter fallen beispielsweise die Religion, der Beruf, der Freundeskreis oder die sexuelle Orientierung. Das Internet kann zur freien Selbstbestimmung beitragen, indem es zum Beispiel die Interaktion mit Menschen auf der ganzen Welt ermöglicht und es somit vereinfacht gleichgesinnte Personen kennenzulernen und sich mit ihnen in Interessengruppen zusammenzuschließen. Darüber hinaus gibt es freie Informations- und Bildungsangebote, die Menschen bei der Entwicklung eines selbstbestimmten Lebensentwurfes unterstützen. Gleichzeitig muss durch die Privatheit jedoch garantiert werden, dass man die Möglichkeit hat zu wählen, welche Informationen man über sich preisgibt und welche nicht.

5.1.2 Demokratische Partizipation

Unter demokratischer Partizipation versteht man die Freiheit des Einzelnen, sich in sozialen und politischen Diskursen frei zu äußern und an der gesellschaftlichen Willensbildung teilzunehmen. Außerdem muss der freie Zugang zu Informationen, die für die politische Willensbildung notwendig sind, gegeben sein. Die demokratische Partizipation ist ein wichtiger Aspekt der freien Selbstbestimmung und auch hier kann das Internet im hohen Maß zu einer politischen Teilhabe beitragen. Politisch gleichgesinnte Menschen können sich einfacher vernetzen und ihre Botschaften nachhaltiger verbreiten und sind dabei nicht auf etalbierte Medien wie das Fernsehen oder Zeitungen angewiesen. Natürlich setzt auch die demokratische Partizipation eine angemessene Privatheit voraus. Eine Meinungsbildung in politischen Gruppen kann nur produktiv erfolgen, wenn ihre Mitglieder darauf vertrauen können, dass ihre Beiträge nicht in einen falschen Kontext geraten. Teilnehmer an politischen Diskursen müssen darüber hinaus nur diejenigen Aspekte ihrer Persönlichkeit zeigen, die für den Diskurs relevant sind. Je nach Kultur ist dies allerdings unterschiedlich, in Deutschland ist beispielsweise die Familie eines Politikers Privatsache während sie in den USA ein wichtiger Bestandteil politischer Selbstdarstellung ist.

5.1.3 Wirtschaftliches Wohlergehen

Das wirtschaftliche Wohlergehen ist eine grundlegende Voraussetzung für ein menschenwürdiges Leben. Das Internet als zentraler Bestandteil der modernen Wirtschaft trägt erheblich zum Wohlstand bei. So ist der Zugang zum Internet in modernen Informationsgesellschaften für alle schon ein Muss. Hier ermöglicht das Internet Teilnahme an Bildung, Wissen und Märkten. Es bietet eine Vielfalt an neuen

Berufsmöglichkeiten und ermöglicht es Unternehmen ihre Ware einfacher international zu verkaufen. Die Privatheit spielt auch hier eine Rolle: Fallen Unternehmen durch Verletzung der Privatheit auf, indem sie beispielsweise persönliche Daten ohne Einverständnis des Nutzers verwenden, so kann dies zu einer Schmälerung des Vertrauens der Kunden in das Unternehmen führen und somit die Entwicklung internetbasierter Wirtschaftszweige verlangsamen.

Das Internet unterstützt die europäischen Werte der freien Selbstbestimmung, der demokratischen Partizipation und des wirtschaftlichen Wohlergehens signifikant. Es erfordert jedoch gleichzeitig einen angemessenen Schutz der Privatheit der Nutzer. Andernfalls kann das Internet eben jene Werte einschränken anstatt sie zu unterstützen. Die Privatheit muss so geschützt werden, dass das Internet seine Möglichkeiten, diese Werte zu unterstützen, entfalten kann.

5.2 Einschränkung der Grundwerte durch Verletzung der Privatheit

Durch die Verletzung der Privatheit können verschiedene Probleme auftreten, welche dazu führen das die oben aufgeführten Grundwerte eingeschränkt werden. Es kann zur De-Kontextualisierung kommen, also persönliche Daten eines Nutzers werden in Kontexten verwendet, denen der Nutzer nicht zustimmen würde. Dies kann zur Einschränkung der freien Selbstbestimmung führen, wenn zum Beispiel private politische Aussagen publik werden und der Nutzer somit in Schwierigkeiten am Arbeitsplatz kommt. Ein weiteres Problem ist die Persistenz der Daten. Persönliche Daten werden länger gespeichert als es nötig ist und Nutzer wissen nicht immer was mit ihren Daten passiert, wenn sie sich von einem Dienst abmelden und diesen nicht mehr nutzen. Diese Daten werden nicht unbedingt immer gelöscht, viele Anbieter anonymisieren sie einfach nur. Das führt zu einem weiteren Problem, nämlich die Re-Identifikation. Liegen genug persönliche Daten vor, so können sie trotz Anonymisierung mittels fortgeschrittener Analysetechniken wieder auf die einzelnen Personen zurückgeführt werden. Diese drei Probleme können in Kombination erhebliche Risiken für die freie Selbstbestimmung und die demokratische Partizipation haben. Werden beispielsweise interne politische Diskussionen einer Interessengruppe öffentlich kann das Wahlverhalten der Gruppenmitglieder hervortreten. Dies beschädigt den demokratischen Grundsatz des Wahlgeheimnisses. Indirekte Effekte können auch sein, dass sich Menschen aufgrund dieser Risiken scheuen das Internet zur Unterstützung eben dieser Werte zu nutzen, womit ein mächtiges Werkzeug der Kommunikation wegfällt.

5.3 Privatheit als Menschenrecht

Als Menschenrecht ist die Privatheit juristisch umgesetzt als Anspruch auf Datenschutz. In Deutschland wird das Recht auf informationelle Selbstbestimmung damit begründet, dass durch die Bedingungen moderner Datenverarbeitung die Selbstbestimmung bei der freien Entfaltung der Persönlichkeit gefährdet werde. Wer nicht wisse, welche Informationen bezüglich seines Verhaltens gespeichert und bevorratet werden, werde aus Vorsicht sein Verhalte aus Angst vor möglichen Folgen anpassen. Dies beeinträchtigt nicht nur die individuelle Handlungsfreiheit, sondern auch das Gemeinwohl, da unsere demokratische Gesellschaft auf die Mitwirkung seiner Bürger angewiesen ist, ohne dass diese Angst vor Überwachungsmaßnahmen und deren Folgen haben müssen.

5.4 Schutzmaßnahmen

In Zeiten des Social Webs ist es wohl das wichtigste, dass ein Verständnis für die Bedeutung der Privatsphäre geschaffen wird. Man sollte Privatheit im Bildungssystem sowie im öffentlichen Diskurs nachhaltig verankern. Bekannte Phrasen wie "Ich habe ja nichts zu verbergen" müssen konsequent widersprochen werden, da sie hochriskant sind. Für einen kompetenten Umgang mit dem Begriff der Privatheit sollte man mehrere Kompetenzen besitzen:

1. Die ethische Kompetenz, nämlich zu wissen warum private Daten als schützenswert einzustufen sind.
2. Die strukturelle Kompetenz, also das Wissen, wer private Daten zu welchem Zweck erhebt und wie diese verarbeitet und weitergegeben werden.
3. Die Risikokompetenz, die Fähigkeit, abschätzen zu können, welche Folgen sich aus der Veröffentlichung bestimmter privater Daten ergeben können.
4. Die rechtliche und technische Kompetenz, also das Wissen über Datenschutzrichtlinien und mögliche Schutzmaßnahmen.

Darüber hinaus gibt es viele einfache Schritte, die man unternehmen kann, um seine Daten besser zu schützen. Man sollte beispielsweise konsequent die Privatsphäre-Einstellungen von sozialen Netzwerken nutzen, seinen Browserverlauf sowie Cookies dauerhaft löschen und den Datenzugriff bei kostenlosen Apps verweigern. Es ist außerdem empfehlenswert bei gängigen Online-Diensten nach Alternativen zu suchen, also Google nicht mehr als Suchmaschine und E-Mail-Dienst in Anspruch nehmen, sondern auf sicherere Plattformen umsteigen, oder von WhatsApp auf andere Messenger, wie Telegram oder Signal umsteigen. Neben den technischen Möglichkeiten besteht auch die Option, sich politisch für den Datenschutz zu engagieren, beispielsweise durch die Teilnahme an Demonstrationen oder Petitionen. Letztendlich sollten in einer Demokratie die Bürger entscheiden.

Datenschutz sollte jedoch nicht nur die Aufgabe der Nutzer sein. Unternehmen, Staat und öffentliche Organisationen sollten sich dazu verpflichten den Grundsätzen der Verhältnismäßigkeit, Informationsgleichheit und Informationsgerechtigkeit bei der Datenerhebung zu folgen. Das Stichwort ist ”Privacy by Design”. Das bedeutet, dass man bereits bei der Entwicklung neuer Technologien darauf achtet, den Umfang der verarbeiteten schützenswerten Daten zu minimieren und transparent zu machen, welche Daten zu welchem Zweck erhoben und weitergegeben werden. Es sollte die Möglichkeit für Nutzer bestehen, sich ohne Vorkenntnisse einfach via Voreinstellungen schützen zu können. Für diesen Privacy by Design Ansatz ist jedoch eine ethische Sensibilisierung der Entwickler notwendig.

5.5 Datenschutz bei Facebook

Als größtes soziales Netzwerk auf der Welt sollte man meinen, Facebook hätte einen guten Datenschutz an Bord, dem ist leider nicht so. Ganz im Gegenteil, Facebook ist seit seiner Gründung immer wieder in den Fokus von Datenschützern gerückt. So bezeichnete der Leiter des Unabhängigen Landeszentrum für Datenschutz Dr. Thilo Weichert Facebooks Strategie mit ”Datenschutzverstoß als Geschäftsmodell”, denn das Unternehmen verstößt in vielerlei Hinsicht gegen Datenschutzvorschriften und ist sich dessen auch sehr bewusst. [8]

So holt Facebook beispielsweise nicht die notwendige Einwilligung seiner Nutzer für die Datenübermittlung ins außereuropäische Ausland ein. Die Einwilligungen, die von Facebook eingeholt werden, genügen oft nicht nicht den datenschutzrechtlichen Anforderungen. Die Allgemeinen Geschäftsbedingungen enthalten verbraucherschädigende und rechtlich unwirksame Klauseln. Eine klare Erkennung der datenschutzrechtlichen Verantwortlichkeiten ist nicht gegeben. Die Pflicht zur vollständigen Löschung persönlicher Daten wird vom Unternehmen nicht umgesetzt. Die Daten Dritter werden ohne Einwilligung und ohne gesetzliche Legitimation verarbeitet. Es kommt zu Profilerstellungen von denen Betroffene nicht in Kenntnis gesetzt werden und auch keine Widerspruchsmöglichkeiten haben. Die pseudonyme oder anonyme Nutzung des sozialen Netzwerkes wird nicht zugelassen. Ein adäquates Minderjährigenschutz wird nicht durchgesetzt. Sogar Inhalte privater Konversationen werden von Facebook unter Verletzung des Telekommunikationsgeheimnisses kontrolliert, angeblich aus Sicherheitsgründen.

Dies ist nur die Spitze des Eisbergs. Als Facebook dann im Mai 2012 an die Börse ging, veröffentlichte das Unternehmen ein Börsenprospekt, in welchem es die Unwägbarkeiten strengerer Datenschutzvorschriften erläuterte. Demnach könnten ungeahnte Kosten entstehen, die Einführung neuer Produkte sich verzögern oder für schlechte Presse gesorgt werden. Dies zeigt, dass sich Facebook durchaus ihrer Datenschutzverletzungen bewusst ist, aber dieses Risiko in Kauf nehmen. Dabei sind Datenschutzverstöße, wenn sie mit Absicht begangen werden, um sich zu bereichern, sogar strafbar. Es stellt sich die Frage, warum Facebooks geschäftsmäßige und systematisch begangenen Datenschutzverstöße nicht als kriminelles Verhalten geahndet werden und schwerwiegende Konsequenzen für das Unternehmen ausbleiben.

5.5.1 Post Privacy

Facebook geht es gar nicht darum, seine Datenschutzverstöße mit technischen Fakten oder rechtlichen Argumenten zu widerlegen, sondern sie wollen einen gesellschaftlichen Wertewandel hin zur Post Privacy. Post Privacy ist die Forderung nach der Aufhebung der rechtlichen Einschränkungen für die Nutzung von Inhalts- und Nutzungsdaten des Internets. Mark Zuckerberg, CEO von Facebook, beteuerte so schon im Januar 2010, dass Menschen sich daran gewöhnt haben, immer mehr Informationen auf viele Arten offener mit anderen und immer mehr Menschen zu teilen. Über die Jahre änderte Facebook in diesem Sinne seine Plattform. Nicht selten gab es Protest gegen die Änderungen, letztendlich nahmen die Menschen aber die datenschutzrechtlich zweifelhaften Veränderungen hin und fanden sie am Ende sogar besser. Darüber hinaus stellt sich Facebook öffentlich oft als einer der ”Guten” dar und behaupten sie sorgen durch ihr Engagement für mehr Offenheit, Demokratie und Transparenz. Angesichts dieses gesellschaftlichen

Auftrages sind Verstöße gegen einzelne nationale oder europäische Gesetze offenbar unvermeidbar und hinnehmbar.

Würde der Forderung nach Post Privacy nachgegeben werden, so würde es den Code zum Gesetz machen. Die Regeln würden von IT-Unternehmen programmiert und letztendlich vom globalen Markt bestätigt werden. Dies ist heute bei Facebook schon oft der Fall. Das Internet ist ein globales Phänomen und Gesetze sind national beschränkt, daher ist es nicht ungewöhnlich, dass ausländische Internetdienste mit deutschem Recht kollidieren. Für Unternehmen wie Google und Facebook ist das in ein Gemeinwohlverständnis interpretierte Konsumverhalten der Nutzer relevant. So hat Facebook beispielsweise einseitig die allgemeinen Geschäftsbedingungen aufgestellt, den Verbrauchern dann zur Kommentierung vorgelegt und dann beschlossen, wenn nicht eine Mehrheit der Nutzer aktiv widerspricht. Dass es zum Widerspruch einer Mehrheit der Nutzer kommt ist unrealistisch und dem ist sich Facebook bewusst. Es gab zwar kein gemeinsames Arbeiten von Facebook und seinen Nutzern an den Geschäftsbedingungen, aber so hat das Unternehmen diese von seinen Nutzern quasi absegnen lassen. So kann Datenschützern, welche sich kritisch äußern, entgegnet werden: "Die machen doch alle freiwillig mit, wo ist das Problem?".

Im Gegensatz zur Post Privacy hat sich in Europa das Konzept Modern Privacy entwickelt. Dieses Konzept hat sich vom Bundesverfassungsgericht, welches angesichts der Digitalisierung zunächst ein Grundrecht auf informationelle Selbstbestimmung und ergänzend ein Grundrecht auf informationstechnische Privatsphäre, also das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, erlassen hat, abgeleitet. In den USA hat der Datenschutz allerdings einen anderen Stellenwert als in Deutschland. Dort hat sich der moderne Datenschutz seit Jahrzehnten nicht weiterentwickelt.

5.5.2 Facebooks Kommunikationsstrategie

In der frühen Phase von Facebook wurden Beschwerden einfach ignoriert oder lösten standardisierte E-Mail-Antworten aus. Es wurden sogar Einzelanfragen von deutschen Aufsichtsbehörden ignoriert, sofern keine direkten Sanktionen zu befürchten waren. In der Kommunikation mit Facebook zeigte das Unternehmen nie eine Änderungsbereitschaft und äußerte immer die selben Argumente. So würde für deutsche Datenschutzbehörden keine Zuständigkeit bestehen, sondern verantwortlich sei wegen der in Dublin sitzenden europäischen Zentrale die irische Datenschutzaufsicht. Darüber hinaus wurde immer wieder betont, dass die Verarbeitung der Daten von Facebooknutzern durch deren Einwilligung legitimiert sei und sich das Unternehmen nicht unzähligen Datenschutzregimes unterwerfen könne, da es international operiert.

Die zentrale Strategie von Facebook ist es, eine verbindliche rechtliche Klärung zu vermeiden, beziehungsweise diese in eine weit entfernte Zukunft hinauszuschieben. Eine solche Klärung wurde bisher noch nicht erreicht und wird derzeit auch nicht durch den irischen Datenschutzbeauftragten angestrebt. Es werden nur Empfehlungen abgegeben und keine Sanktionen ausgesprochen.

Allen Anschein nach besteht bei der Illegalität beim Datenschutz kein Grund zur Einstellung einer einträglichen Praxis, um gegen die vielen Verstöße vorzugehen. Es bräuchte wahrscheinlich einen gesellschaftlichen Aufschrei und Empörung über die Vorgehensweise die Facebook seit seiner Gründung bezüglich des Datenschutzes verfolgt. Das Unternehmen versteht es allerdings sehr gut, sich der gesellschaftlichen Ächtung zu entziehen und steht heute in den Augen vieler eher positiv als negativ da.

6 Zukunft der Privatheit

Wie es in Zukunft um die Privatheit im Internet steht, ist sehr fraglich und nicht absehbar. Die deutsche Akademie der Technikwissenschaften acatech hat sich mit der Frage auseinandergesetzt, was es braucht, um die Privatheit im Internet nachhaltig umzusetzen. [9] Sie kommt zu dem Schluss, dass Nutzer einerseits über die Möglichkeiten des Internets und seinen Risiken aufgeklärt werden müssen und andererseits darauf vertrauen können müssen, dass Internetdienste ihre Privatheit respektieren und entsprechenden Umgang mit ihren Daten pflegen. Dazu wurden eine Reihe von Handlungsempfehlungen in Bildung, Recht, Wirtschaft und Technik aufgestellt, die ihn Zukunft dazu beitragen sollen, dass sich eine Kultur der Privatheit entwickelt.

6.1 Bildung

Die Bildung spielt eine entscheidende Rolle für die Etablierung einer Privatheitskultur. Da das Internet gegenwärtig die wichtigste Kulturtechnik ist, sollten auch umfangreiche Kenntnisse und Handlungskompetenzen für den Umgang mit dem Internet vermittelt werden. Die Entwicklung einer Internetkompetenz

muss ein neues Bildungsziel werden und sollte den selben Stellenwert wie etablierte Schulfächer bekommen. Es ist wichtig über wichtige Geschäftsmodelle und relevante Privatheitsrisiken im Rahmen der schulischen Laufbahn aufgeklärt zu werden. Ziel sollte es sein anhand der erlangten Erkenntnisse eigenständig in der Lage zu sein, für sich Privatheitspräferenzen zu bestimmen und umzusetzen.

Um dieses Ziel zu erreichen sollte, Bildung für Internetkompetenz flächendeckend verfügbar sein. Nicht nur für Schulen sollte dieses Fach obligatorisch sein, sondern Menschen jeder Berufsgruppe sollten Zugang zu diesem Wissen bekommen. Menschen, die in Berufen arbeiten, die besonders mit dem Thema zu tun haben, sollten spezielle Weiterbildungsmaßnahmen in Anspruch nehmen können. Darüber hinaus sollte der Privatheitsschutz fester Bestandteil der Ausbildung bei Berufen sein, vor allem jene, die direkt oder indirekt mit Privatheit zu tun haben, vom Arzt bis zum Fachinformatiker. Wichtig ist auf die Verfügbarkeit in Studiengängen, in denen zukünftige Führungskräfte ausgebildet werden.

Neben der direkten Verankerung im Bildungssystem sollte das Thema Privatheit auch durch öffentliche Kampagnen in den gesellschaftlichen Diskurs gebracht werden. Aktionstage wie der "Safer Internet Day" der EU könnten sich auch dem Thema Privatheit widmen. Des Weiteren sollten die Forschungsanstrengungen zu Privatheitsvorstellungen und -praktiken ausgebaut werden. Inwieweit haben sich die Vorstellungen und Praktiken der Privatheit über die Jahre geändert? Wie sehen die alltäglichen Privatheitspraktiken von Nutzern aus? Forschungen in diesem Bereich sollten dauerhaft stattfinden, da technologische Neuerungen keine Seltenheit sind und mit ihnen immer wieder neue Anforderungen an die Privatheit gestellt werden. Zusätzlich wird vorgeschlagen Sozial- und Technikwissenschaften für die Forschung zusammenzuführen. So soll beispielsweise die schulische Vermittlung von Internetkompetenzen durch pädagogische und sozialwissenschaftliche Forschungsbemühungen verfolgt werden, um ihre Effektivität zu bestimmten.

6.2 Recht

Das Recht soll das Vertrauen der Menschen im Internet stärken, indem sie einen bewussteren Umgang mit ihm ermöglichen und dessen Vertrauenswürdigkeit erhöhen. Da es sich bei dem Internet um ein globales Phänomen handelt, wäre eine international gültige oder wenigstens sehr weitreichende Rechtsordnung optimal.

Gesetze und Verordnungen sollen nur Ziele formulieren und nicht in die technische Umsetzung von Diensten eingreifen. Die Art und Weise der Umsetzung sollte bei den Anbietern liegen, um Einschränkungen zu minimieren. Auf die Einhaltung der Ziele muss der Dienst natürlich geprüft werden. Dienstanbieter sollten Privatheitsschutzrechte aus den Herkunftsländern der Nutzer implementieren. Da eine internationale Rechtsordnung nicht in Aussicht steht, ist es angebracht auf die Rechte aus den jeweiligen Ländern zu achten, auch um den Nutzer nicht mit anderen Regeln zu verwirren. Realisierbar wird solch ein Vorhaben allerdings erst, wenn man die Privatheitsschutzrechte möglichst weiträumig vereinheitlicht. Des Weiteren sollten die Einwilligungen reguliert werden. Nutzer sollten genau wissen, was sie zustimmen, wenn sie ihr Einverständnis für die Erhebung und Verwendung persönlicher Daten geben. Eine Verarbeitung von persönlichen Daten ohne Zustimmung des Nutzers sollte nur erfolgen, wenn entsprechende Schutzmaßnahmen ergriffen werden, beispielsweise durch Verschlüsselung.

Ein wichtiger Aspekt ist also die Schaffung von Transparenz und die Ermöglichung von Kontrolle. Dienste sollten von Anfang an verständlich darstellen, welche persönlichen Daten sie speichern, was mit ihnen geschieht, an wen sie weitergeben werden und wie lange sie aufbewahrt werden. Nutzer sollten die Kontrolle über ihre Daten haben, also befugt sein, sie zu korrigieren und zu löschen. Neben einer aktiven Löschung von Daten sollte es auch Möglichkeiten geben Fristen einzustellen, nach denen persönliche Daten automatisch gelöscht werden. Es sollte dem Nutzer ebenfalls möglich sein, seine persönlichen Daten in andere Netzwerke migrieren zu können. Nutzt man ein soziales Netzwerk über einen längeren Zeitraum, so wird der Nutzer in einem hohen Maße an diese Plattform gebunden. Würde seitens der Betreiber die Möglichkeit bestehen seine Daten zu migrieren, so könnte man sehr einfach auf einen anderen Anbieter umsteigen und dabei seinen persönlichen Kontext mitnehmen. Dies ist nicht nur für den Nutzer positiv, es würde auch einen faireren Wettkampf zwischen verschiedenen sozialen Netzwerken ermöglichen.

Ein weiterer wichtiger Punkt ist Einhaltung zentraler Datenschutzprinzipien. Dazu gehören Zweckbindung, Datenminimierung, Datensicherheit und privatheitsschutzfreundliche Voreinstellungen. Diese Prinzipen müssen von den Diensten eingehalten werden. Ein Mittel, um die Einhaltung dieser Prinzipien zu garantieren und Dienste auf diesen Aspekt untereinander zu vergleichen, könnten Zertifikate sein. Eine weitreichende, am besten internationale, Etablierung von Zertifikaten und Prüfsiegel könnte erreichen, dass der Schutz der Privatheit ebenfalls zu einem Wettbewerbsvorteil wird und Internetdienste sich dementsprechend mehr Mühe bei der Ausgestaltungen ihres Datenschutzes machen.

6.3 Wirtschaft

Die Wirtschaft soll zu einer Privatheitskultur beitragen, indem Dienstleister Transparenz schaffen, Kontrolle und Migration ermöglichen sowie Datenschutzprinzipien beachten. Man könnte neben dem "bezahlen" mit persönlichen Daten beispielsweise auch eine Art kostenpflichtigen Dienst anbieten, welcher dann restriktiver mit persönlichen Daten umgeht, also diese beispielsweise nicht für gezielte Werbung einsetzt oder die pseudonyme und anonyme Nutzung erlaubt. Darüber hinaus sollten Dienste die Verwendung von sogenannten Privacy Agenten ermöglichen. Privacy Agenten sind Programme, welche vom Nutzer einmalig eingestellt werden und fortan die Privatheitseintstellungen automatisch übernehmen. Diese Technik setzt allerdings voraus, dass Dienste die relevanten Informationen in einem Format bereit stellen, welches von diesen Agenten genutzt werden kann. Für diesen Zweck sowie für die Migration von Daten könnten Standards vereinbart werden. Unternehmen sollten außerdem verpflichtet werden Privatheitssiegel und -zertifikate zu nutzen. Diese sollten unabhängig sein und regelmäßigen Qualitätsprüfungen unterworfen sein.

6.4 Technik

Die Empfehlungen aus Bildung, Recht und Wirtschaft sind oft nur mit entsprechender technischer Unterstützung realisierbar. Diese ist aber, wenn überhaupt nur ansatzweise vorhanden, muss also unbedingt dahingehend ausgebaut werden. Internetdienste sollten außerdem nach dem "Privacy by Design" Prinzip entwickeln. Normalerweise werden Dienste zunächst im Hinblick auf ihre Funktionalität entwickelt und Sicherheits- sowie Privatheitsmaßnahmen erst später realisiert. Dadurch gestaltet sich die Implementierung des Datenschutzes schwieriger. Stattdessen sollte man den Maßnahmen eine höhere Priorität zu weisen und diese während der Entwicklung sowie der Betreibung des Dienstes strikt beibehalten. Anstatt sich auf die Funktionalität zu fokussieren, sollte man zunächst eine Diskussion und Analyse über den Einfluss des Dienstes auf die Privatheit seiner Nutzer durchführen.

Es sollten technische Möglichkeiten für die Probleme der anderen Bereiche, wie beispielsweise die Einwilligung zum Erheben und Verarbeiten privater Daten sowie der Nutzerfreundlichkeit, erforscht werden. Eine Einwilligung sollte technisch so gestaltet werden, dass Nutzer sie tatsächlich bewusst geben und nicht blindlings zustimmen. Die Nutzerbarkeit von Technologien, welche die Privatheit schützen sollte verbessert werden, da diese Technologien oft mit dem Bedürfnis einen Dienst auf möglichst einfache Art und Weise zu bedienen kollidieren. In diesem Zusammenhang sollte man auch die Frage nach dem Vergessenwerden im Internet erforschen. Methoden, die es ermöglichen, weitergegebene Daten und durch Auswertung gewonnene Informationen zu löschen sollten erforscht und entwickelt werden.

Die Nutzungskompetenzen und Gestaltungsmöglichkeiten der Nutzer können durch die Weiterentwicklung von Werkzeugen, die den Nutzern zeigen, welche persönlichen Informationen ein bestimmter Dienst oder eine Gruppe von Diensten kennt und was das angesichts ihrer Privatheitspräferenzen bedeutet, unterstützt werden. Hier können Standards entwickelt werden, nach denen sich die Anbieter bei der Verarbeitung persönlicher Daten richten müssen und mittels dessen dann Nutzerprofile für den Umgang mit Privatheit entsprechend dieser Regeln erstellt werden können. Diese Standards könnten auch Formate für die Migration von Nutzerprofilen von einen Dienst in einen anderen beinhalten.

Neben den Standards für die Dienste sollten auch Standards entwickelt werden für Auditierungen und Zertifikate. Mittels dieser Maßnahmen können Dienste einfacher auf den Schutz der Privatheit geprüft werden. Prozesse, Bewertungskriterien und Zertifikate werden durch die Standardisierung vergleichbar und somit können Dienste besser nach ihrem Respekt für die Privatheit der Nutzer klassifiziert werden. Außerdem sollten Dienste, welche Informationen wie den Klarnamen der Nutzer nicht zwingend benötigen auch eine anonyme beziehungsweise pseudonyme Nutzung zulassen. Nutzer können hier auch anhand anderer Eigenschaften verifiziert werden, beispielsweise durch das Alter oder den Standort.

Des Weiteren ist es wichtig grundlegende Methoden und Technologien weiterzuentwickeln um zukünftigen Sicherheitsansprüchen gerecht zu werden. Vor allem die Entwicklung kryptographischer Verfahren, welche auch neuen Bedrohungen standhalten, ist wichtig für den Datenschutz. Um das Problem von Schwarzmärkten im Internet zu bekämpfen, wäre es auch sinnvoll, Methoden zu entwickeln, welche einerseits die Privatheit schützen, andererseits aber auch die Zurechenbarkeit von illegalen Handlungen erlauben.

Letztendlich ist hier auch eine Auseinandersetzung mit verschiedenen Dualitäten wie privatheitsfreundlich und privatheitsunfreundlich, sicher und unsicher oder privat und öffentlich sinnvoll. Diese Dualitäten halten oft nicht mehr mit dem modernen Stand der Technik mit. Hier stellt sich die Frage inwieweit diese Dualitäten differenziert als hinreichend für einen bestimmten Kontext bewertet werden können. Dieses Problem versucht beispielsweise das Konzept der Privatsphäre im Kontext zu lösen.

7 Privatsphäre im Kontext

Mit der fortschreitenden Digitalisierung ist es notwendig den Begriff der Privatsphäre neu zu denken. Die Zweiteilung in öffentlich und privat war in der analogen Vergangenheit eine nützliche Trennung. Allerdings führt das Social Web zu einer derartigen Vermischung von privat und öffentlich, dass diese Zweiteilung nicht mehr genügt. Die digitalen Informationstechnologien haben die Bedingungen für die Privatsphäre grundlegend geändert. So beginnt die Suche nach einem neuen Bezugssystem für den Begriff der Privatsphäre, der ohne die Sphärentrennung in öffentlich und privat funktioniert. Ein Konzept dafür ist die sogenannte "Privatsphäre im Kontext" von Helen Nissenbaum. [10]

7.1 Bezugssystem

Das Bezugssystem betrachetet die Unversehrtheit des Kontextes. Das Recht auf den Schutz der Privatsphäre ist hier weder ein Recht auf Geheimhaltung noch ein Recht auf Kontrolle, sondern ein Recht darauf, dass der Fluss persönlicher Informationen situationsgerecht, also angemessen ist. Die grundlegenden Bestandteile für dieses Bezugssystem sind der soziale Rahmen und die informationellen Normen innerhalbe dieses Rahmens. Ein Verstoß gegen die informationellen Normen stellt dabei eine Übertretung der Privatsphäre dar. Es wird versucht ein komplexes Netz von Beschränkungen für den Fluss persönlicher Informationen zu entwickeln, das ein Gleichgewicht zwischen den verschiedenen Bereichen, also den unterschiedlichen Kontexten des gesellschaftlichen und politischen Lebens herstellt.

7.2 Kontext

Hinter der Idee eines gesellschaftlichen Kontextes verbirgt sich nichts anderes als die Tatsache, dass sich Menschen zueinander unterschiedlich verhalten, je nachdem in welcher sozialen Lage sie sich befinden. Sie handeln dabei in Rollen, die durch gesellschaftliche Felder herausgebildet werden. Es gibt unterschiedliche gesellschaftliche Bereiche, wie Politik, Markt, Arbeit, Staat, Schule oder Familie, welche sich durch unterschiedliche gesellschaftliche Aufgaben auszeichnen und deren genaue Bedeutung den jeweiligen Bereichen nach einem festen Set von Regeln zugeordnet wird. Man kann Kontexte nach der Stärke ihrer institutionellen, allgemeinen oder offiziellen Anerkennung unterscheiden. In gesellschaftlichen Kontexten gelten Gesetze als Methode zur Kontrolle eines Kontextes und gegebenfalls zum Verhängen von Sanktionen. Neben Gesetzen können zur Kontrolle beispielsweise auch Satzungen eines Berufs, eines Vereins oder einer Religionensgemeinschaft gehören. Die unterschiedlichen Methoden können dabei auch zusammenwirken und ineinander greifen. Die unterschiedliche Vermischung von ausdrücklichen und offiziell festgelegten Normen ist die Ursache für Meinungsverschiedenheiten über Art und Reichweite des Schutzes der Privatsphäre. In manchen Fällen können sich Kontexte sogar überschneiden, zum Beispiel sollte ein Arzt seinen Patienten über seine ungesunde Ernährung warnen, ist er aber gerade in einem Kontext als Freund des Patienten anwesend, so würde ein solcher Rat bevormundend wirken und ein Eingriff in die Privatsphäre darstellen.

7.3 Normen und ihre Struktur

Für die Normen gibt es vier Schlüsselelemente:

1. Ein Element mit Vorschriftcharakter.
2. Ein Subjekt, für das die Norm gilt.
3. Eine normative Handlung, also eine in der Norm festgelegte Art zu handeln.
4. Eine Bedingung für ihre Anwendung, also die Umstände, unter denen vom Gegenstand der Norm erwartet wird, dass er normativ handelt.

Die Normen sind dabei weitestgehend in Systeme wie Gesetze, Spielregeln, Satzungen oder Prinzipien eingebettet.

Kontextbezogene, informationelle Normen werden von vier wesentlichen Kennwerten bestimmt: Kontext, Handelnde, Merkmale und Grundsätze der Übermittlung. Sie definieren um welche Information es geht, für wen sie bestimmt ist, wer die Information ausgibt und sie empfängt sowie die Grundsätze, nach denen die Information übertragen wird. Die Normen steuern also gemäß der Übertragungsgrundsätze den Fluss bestimmter Arten von Informationen über einen Informationsgegenstand von einem Handelnden zu einem oder mehreren anderen Handelnden, welche alle eine bestimmte Funktion oder Rolle einnehmen.

7.4 Akteure

Kontextbezogene Informationsnormen berücksichtigen drei verschiedene Arten von Handelnden: Die Sender von Informationen, die Empfänger von Informationen und den Gegenstand der Information. Für die Ausführung der Normen ist es essentiell die kontextbezogenen Rollen aller drei Akteure soweit wie möglich zu bestimmen, je mehr Informationen zu den Akteuren vorhanden ist, desto einfacher und besser gelingt später die Entscheidung über mögliche Privatsphäreverletzungen. Die Rolle der Handelnden ist eine der entscheidendsten Variablen, die Einfluss darauf haben, ob Menschen mit ihren vielschichtigen Befindlichkeiten glauben, ihre Privatsphäre sei verletzt worden oder nicht.

7.5 Attribute und Arten von Informationen

Für die Normen ist es entscheidend Wissen über die Art oder das Wesen von Informationen zu besitzen. Der Informationsfluss kann je nach Art der Information unterschiedlich eingeschränkt sein und anderen Regeln unterliegen. Zum Beispiel werden Informationen im Gesundheitswesen je nach Art unterschiedlich eingeschränkt. Informationen über die Adresse oder die Telefonnummer eines Patienten werden anders behandelt als Informationen über den Gesundheitszustand des Patienten. Die Unversehrtheit des Kontextes kennt hier also theoretisch eine unbegrenzte Anzahl von Möglichkeiten anstatt nur privat und öffentlich. Die Normen können bestimmte Merkmale in bestimmten Kontexten passend oder unpassend machen, ob etwas angebracht ist oder nicht, wird weder eindimensional noch dual entschieden.

7.6 Übertragungsgrundsätze

Ein Übertragungsgrundsatz ist eine Einschränkung des Informationsflusses bezüglich seiner Verteilung, seiner Verbreitung und seiner Übertragung von einer Partei zu einer anderen innerhalb eines konkreten Kontextes. Die Werte der Übertragungsgrundsätze formulieren dabei bestimmte Bedingungen oder Zustände, unter denen Übertragungen stattfinden dürfen oder nicht. Die Übertragungsgrundsätze zeichnen sich durch Folgende Merkmale aus:

- Vertraulichkeit, die Empfängerpartei darf die Informationen nicht weitergeben.
- Wechselseitigkeit, der Grundsatz, dass Informationen in beide Richtungen fließen sollen.
- Anspruch, regelt ob jemand bestimmte Informationen verdient hat.
- Berechtigung, die darüber entscheidet, ob jemand berechtigt ist, etwas zu wissen.
- Zwang, der dafür sorgt, dass eine Partei gezwungen oder verpflichtet wird ist, anderen Personen Informationen zugänglich zu machen.
- Notwendigkeit, die bestimmt, dass eine Partei Informationen einer bestimmten Art benötigt.

7.7 Unversehrtheit des Kontexts

Schlussendlich kann man nun die Unversehrtheit des Kontexts als Entscheidungsgrundlage anstelle vom Schutz der Privatsphäre nutzen. Das Konzept kann als Entscheidungsmechanismus angewendet werden, um festzustellen ob ein Verstoß stattgefunden hat oder nicht. Problematische neue Vorgehensweisen, die sich durch den Einsatz neuer technischer Geräte oder Systeme ergeben können mit dem Konzept bewertet werden, indem man übereinkommene Gepflogenheiten mit der neuen Verfahrensweise vergleicht und herausfindet welche Normen die Oberhand haben. Des Weiteren muss man untersuchen, ob die neue Verfahrensweise ändert wer Informationen empfängt, um wen es geht und wer die Informationen übermittelt. Ebenfalls muss festgestellt werden, ob sich die Art der Information sowie die Grundsätze der Übertragung geändert haben.

8 Freiheit versus Sicherheit

Mit dem 11. September 2001 rückte die Sicherheitsdebatte in den Fokus und verankerte sich mit der immer größer werdenden Gefahr des internationalen Terrorismus auf die Tagesordnung der Bundesregierung. Streitpunkt in der Debatte ist immer wieder das Spannungsfeld zwischen staatlicher Kontrolle und den individuellen Bürgerrechten. Mit dem Aufkommen und der massiven Verbreitung des Internets hielt auch der Datenschutz in diesem Spannungsfeld Einzug. [11]

8.1 Recht auf Sicherheit

Der Schutz vor Kriminalität und terroristischen Anschlägen ist Teil der Verantwortung eines Staates. Genau aus diesem Grund haben sich Menschen zum gegenseitigen Schutz ihres Lebens, ihrer Freiheit und ihres Vermögens zusammengeschlossen in einem Staatswesen. Damit verzichten sie zu Gunsten des staatlichen Gewaltmonopols auf Selbsthilfe, also auf den eigenen Gebrauch von Gewalt.

Vor allem in Folge des 11. Septembers wurden so im Namen der Sicherheit immer wieder neue Gesetze gemacht. Schärfere Kontrollen und härtere Strafen werden durch den Terror der letzten Jahre legitimiert. Die Sehnsucht nach Sicherheit wächst mit der Angst in der Gesellschaft und Gesetze, die in ruhigen Zeiten nie akzeptiert werden würden, können so ihren Platz einnehmen. So sorgte das Terrorismusbekämpfungsgesetz anfang 2013 für den Ausbau der Kontrollmöglichkeiten für den Kampf gegen den internationalen Terrorismus. Darüber hinaus gestattet das Gesetz den Datenaustausch zwischen den Behörden, die Verbesserung von Grenzkontrollen, die Schaffung der Rechtsgrundlagen für die Aufnahme biometrischer Merkmale in Pässen und Personalausweisen und die Rasterfahndung mit Einbezug bestimmter Sozialdaten. Das Hauptargument für solch eine Verschärfung der Sicherheitspolitik bleibt dabei meistens gleich: Man müsse den neuartigen Terror bekämpfen, dieser hat die Möglichkeit des Einsatzes von Massenvernichtungswaffen, biologischen Kampfstoffen und Giftgasen. Angesichts dieser Gefahren können neue Gesetze stets legitimiert werden.

8.2 Prävention oder Freiheitsentzug

Das Staatsziel der vorbeugenden Verbrechensbekämpfung der inneren Sicherheit steht im Spannungsverhältnis zur Rechtsstaatlichkeit liberaler Prägung. Gemeint ist hier vor allem die Freiheitsrechte des Beschuldigten, wie das Gebot des fairen Prozesses, die Unschuldvermutung und das strenge Beweisrecht sowie auch der Respekt der Intim- und Privatsphäre. Konkret geht es darum wie weit diese rechtsstaatlichen Garantien aufgehoben werden für die Durchsetzung frühzeitiger Maßnahmen der Gefahrenabwehr. Der Respekt der Freiheitsrechte schützt nicht nur unschuldig in Verdacht geratene Menschen, sondern alle Menschen vor Vor- und Fehlurteilen einer selbstgerechten Sicherheitsbehörde und der Gerichte.

Je mehr Maßnahmen der Überwachung es gibt, desto mehr wird denen die die Verdächtigen schützen die Kontrolle entzogen. Moderne Ermittlungsverfahren erfassen nicht nur Verdächtige einer Straftat. Mittels Rasterfahndung werden beispielsweise Daten einer großen Menge von Personen durchforstet, die nichts mit der Polizei zu tun haben und auch nicht als Störer oder als gefährlich qualifiziert werden können. Die Rasterfahndung nimmt also einen erheblichen Eingriff in die Datenschutzgrundrechte vor. Je weiter Ermittlungsinstrumente auf unbeteiligte Dritte ausgeweitet werden, desto schneller verliert die Kategorie des konkreten Tatverdachts ihre legitime und begrenzende Kraft. Das Freiheitsrecht des Beschuldigten trifft auf das Interesse an einer funktionstüchtigen Strafrechtspflege. Die Frage ist, wie diese gegenläufigen Prinzipien auszulegen sind. Führt man sich die neue Dimension, die der internationale Terrorismus über die letzten Jahre angenommen hat, vor Augen, so wird klar, dass man nicht schlicht die Freiheitsrechte des Bürgers den Vorrang einräumen kann. Das Bedürfnis nach kollektiver Sicherheit und das individuelle Freiheitsrecht müssen also in einer Art und Weise in ein Verhältnis zueinander gebracht werden, dass diese beiden im Widerspruch stehenden Verfassungswerte in einer idealen Kombination zueinander stehen. Ziel ist ein maximales Maß an Freiheit, gewährleistet durch eine optimale Sicherheit. Das große Problem ist, dass es hier keinen Maßstab gibt, solch eine Balance ist nicht einfach zu finden. Nach dem 11. September wurde mit dem Sicherheitspaket II versucht solch eine Balance zu finden und es hat sich prompt gezeigt, wie unterschiedlich Experten das beschlossene Verhältnis zwischen Freiheit und Sicherheit bewerten. Auf der einen Seite wird das Pakte als eine gute Verbindung zwischen kollektiver Sicherheit und individueller Freiheit gesehen, auf der anderen Seite sah man den Weg in den Überwachungsstaat.

8.3 Folgen für die Politik

Da es in diesem Spannungsfeld nur ein abstraktes Ziel, nämlich ein maximales Maß an Freiheit durch optimale Sicherheit, gibt und kein konkreter Weg vorgegeben ist, müssen die Maßnahmen zur Terrorismusbekämpfung auf unterschiedliche Gesichtspunkte hin befragt werden. Man muss sich Fragen, ob die Maßnahmen überhaupt geeignet sind, den Terrorismus erfolgreich zu bekämpfen, ob die damit verbundene Einbuße an Freiheit in einem angemessenen Verhältnis zur Schwere des Eingriffs steht und ob die beabsichtigten Maßnahmen möglicherweise mit nicht wünschenswerten Nebenfolgen verknüpft sind.

Darüber hinaus schützt der Respekt der Freiheitsrechte nicht nur vor Vor- und Fehlurteilen, sondern ist enorm wichtig für den demokratischen Prozess. In einem Klima der Überwachung und Bespitzelung kann kein demokratischer Prozess gedeihen. Der Grenzverlauf zwischen einem Rechtsstaat und einem

Präventionsstaat lässt sich nicht eindeutig bestimmten, hier gibt es Grauzonen und schleichenden Übergänge hin zum Polizei- und Überwachungsstaat. Wenn der Staat seine eigenen Bürger biometrisch vermisst sowie datenmäßig rastert und erfasst, gefährdet er die demokratisch politische Kultur, welche von Meinungsvielfalt und Engagement der Bürger lebt. Wenn Menschen anfangen andere Menschen aufgrund von bestimmten Rastern zu meiden, wird das Zusammenleben unterschiedlicher Menschen geschädigt, national sowie international. Meinungsvielfalt kann sich so nicht entwickeln und die Demokratie wird geschwächt.

Das Motto der Politik scheint in den letzten Jahren immer wieder "Im Zweifel für die Sicherheit" zu sein. Sicherheitsmaßnahmen werden ausgebaut, Sicherheitsdienste bekommen immer mehr Befugnisse und Ressourcen und die Polizeigewalt nimmt zu. Die neuen Sicherheitsregelungen, die ohne die bestehende Gefahr niemals umgesetzt werden könnten, bleiben dann oft in Zeiten geringster Bedrohung dennoch bestehen und werden nicht zurückgenommen. So verlieren Demokratien über die Zeit immer mehr an Freiheit. Die individuelle Freiheit ist ein Kernelement von Demokratien und ein Hauptunterschied zu Autokratien. Opfert man in Zukunft weiterhin Freiheit zugunsten der Sicherheit, wie lange kann unsere Demokratie dann noch bestehen?

8.4 Neue Gesetze und der Datenschutz

In Folge der immer strengeren Sicherheitspolitik im Inneren wurden eine Reihe an Gesetzen über die letzten Jahre verabschiedet, welche oft von Kritik seitens Datenschützern und Menschenrechtlern überschattet werden. Während sich auf der einen Seite der Bundesinnenminister de Maizière für eine flächendeckende biometrische Videoüberwachung des offline Raums einsetzt und die aktuellen Tests dieser Überwachung am Berliner Bahnhof Südkreuz besucht [12], wächst auf der anderen Seite die Anzahl neuer Gesetze zur Überwachung im Internet. Im Folgenden gehe ich auf drei neue, sehr kontroverse Gesetzgebungen aus diesem Jahr und deren Verhältnis zum Datenschutz ein.

8.4.1 Staatstrojaner

Vor einigen Monaten hat der Bundestag eines der weitreichendsten Überwachungsgesetze in der Geschichte der Bundesrepublik beschlossen. [13] Es bietet Ermittlungsbehörden die Möglichkeit private Computer, Laptops, Handys, Tablets und andere IT-Geräte mit dem sogenannten Staatstrojaner zu infizieren, um die Kommunikation direkt an der Quelle zu überwachen. Das Bundeskriminalamt hatte diese Möglichkeit bereits vor diesem Gesetz mit der Begründung der Gefahrenabwehr von internationalem Terrorismus. Nun wurde sie auf alle Behörden ausgeweitet und kann auch für ganz normale Strafverfolgung genutzt werden. Das Überwachungsgesetz war stets von Streitigkeiten überschattet. So wurde sich oft darüber gestritten, ob es überhaupt eine Rechtsgrundlage für das Vorhaben gäbe. Darüber hinaus werfen Kritiker dem Gesetz einen intensiven Eingriff in die Grundrechte vor. Die Kritik gilt vor allem dem Sachverhalt, dass die Ermittlungsbehörden nicht nur Geräte von Verdächtigen durchsuchen dürfen, sondern auch Geräte anderer Personen. Die Entscheidung erfolgt hier nach eigenem Ermessen der Ermittler. Diese können dann private Chats, beispielsweise in WhatsApp, mitlesen oder auf die gesamten Inhalte von Festplatten zugreifen. Um eine öffentliche Debatte über dieses neue Überwachungsgesetz klein zu halten wurde es in einem bereits existierenden Gesetzesprozess versteckt.

8.4.2 Netzwerkdurchsetzungsgesetz

Das Netzwerkdurchsetzungsgesetz wurde gegen Hasskommentare im Internet und zur Durchsetzung gesellschaftlicher Regelungen im sozialen Netz erarbeitet. Kritiker sehen in dem Gesetz eine Gefahr für die Meinungsfreiheit. [14] Laut dem Gesetz sind soziale Netzwerke dazu verpflichtet offensichtlich rechtswidrige Inhalte innerhalb von 24 Stunden nach Eingang einer Beschwerde zu entfernen. Das Problem hier ist, dass mit nicht Befolgen des Gesetzes Bußgelder drohen. So kommt durch Furcht vor sogenannten "Overblocking" auf. Das bedeutet, dass Betreiber von sozialen Netzwerken dazu geneigt sind lieber zu viel zu löschen als zu wenig. Laut Tobias Gostomzyk, Professor für Medienrechte an der TU Dortmund, ist das Gesetz aufgrund dieses Problems nicht verfassungskonform. Auch Reporter ohne Grenzen sehen hier ein schwerwiegendes Problem mit dem Gesetz.

Das Gesetz erfuhr im Laufe der Zeit mehrere Überarbeitungen und Nachbesserungen. So wurde nun klar definiert, was eigentlich alles unter den Begriff "soziales Netwerk" fällt. Bei älteren Gesetzesentwürfen wären sogar Messenger-Dienste wie WhatsApp unter den Begriff gefallen, was von Datenschützern überaus problematisch gesehen wurde, da diese Dienste überwiegend zur verschlüsselten, privaten Kommunikation in kleineren geschlossenen Gruppen genutzt werden. Des Weiteren war in älteren Entwürfen des Gesetzes,

dass seine Regelung nur gelten, wenn ein soziales Netzwerk mehr als zwei Millionen Nutzer habe. Kritikpunkt war der schwammige Begriff Nutzer: Waren damit einfach nur die Besucher der Seite gemeint oder auch nur registrierte Nutzer? Im finalen Gesetzesentwurf steht nun "registrierte Nutzer". Dennoch geht daraus nicht hervor, inwiefern Karteileichen, Bots oder Nutzer mit mehreren Accounts behandelt werden. Außerdem soll gegen das Overblocking eine "regulierte Selbstregulierung" eingerichtet werden für "nicht offensichtliche" rechtswidrige Inhalte. Die Aufsicht über diese Selbstkontrolleinrichtung sollte dem Bundesamt für Justiz übertragen werden. Dies stößt vor allem mit Blick auf den Grundsatz der Freiheit der Medien auf verfassungsrechtliche Bedenken. Obwohl das Gesetz von einem breiten Bündnis aus Industrie und netzpolitischen Vereinen abgelehnt wurde, wurde es schlussendlich dennoch verabschiedet.

Zahlreiche Gutachten, unter anderem auch vom Wissenschaftlichen Dienst des Bundestage, bescheinigten dem Gesetz neben gravierenden rechtstechnischen Mängeln auch Verstöße gegen das Europarecht und das Grundgesetz. Beispielsweise verletzt das Gesetz das in der E-Commerce-Richtlinie verankerte Herkunftsprinzip. Laut diesem Prinzip müssen sich Dienstanbieter aus dem europäischen Ausland in Deutschland grundsätzlich keinen anderen Regeln unterwerfen als denen des Mitgliedstaates indem sie ihren Sitz haben. [15]

8.4.3 Neues Datenschutzgesetz

Das neue Datenschutzgesetz soll zur Anpassung des deutschen Rechts an die neuen Vorgaben dienen, auf die sich die Mitgliedstaaten der EU und das EU-Parlament im Frühjahr 2016 geeinigt haben. Zu den neuen Vorgaben gehören die Datenschutzgrundverordnung (DSGVO) und die Datenschutzrichtlinie für Polizei und Justiz. Die Datenschutzrichtlinie muss komplett in deutsches Recht umgewandelt werden, die Datenschutzverordnung hingegen tritt für alle Mitgliedstaaten unmittelbar in Kraft, enthält allerdings eine Menge Öffnungsklauseln für nationale Sonderregelungen. Diese Öffnungsklauseln werden laut Kritikern von der Großen Koalition erheblich für Alleingänge ausgenutzt. Das Gesetz soll sogar dort eigene Regelungen enthalten, wo kein Spielraum vorgesehen ist. So soll das Gesetz europarechtswidrige sowie datenschutzfeindliche Positionen beinhalten. [16]

Dies sind die zentralen Kritikpunkte am neuen Datenschutzgesetz:

- Noch schlechtere Kontrolle von Geheimdiensten und Behörden:

  Die Aufsichtskompetenzen der Bundesdatenschutzbeauftragten im öffentlichen Bereich sollen geschwächt werden. Dies betrifft die Kontrolle von Geheimdiensten, Polizei und anderen Behörden. Dieses Vorhaben verstößt gegen EU-Vorgaben. Des Weiteren soll der Bundestag zukünftig nicht mehr proaktiv über Missstände beim Bundesnachrichtendienst informieren.

- Geschwächte Datenschutzaufsicht bei Krankenhäusern, Arztpraxen und Anwaltskanzleien:

  Die Datenschutzkontrolle bei Berufsgeheimnisträgern soll eingeschränkt werden. Den Kontrollbehörden kann nun der Zutritt zu Geschäftsräumen sowie die Aushändigung von für die Kontrolle notwendigen Daten verwehrt werden. Dies gilt außerdem auch für Apotheken, Steuerberatungs- und Buchführungsbüros sowie für Unternehmen der privaten Kranken-, Unfall- oder Lebensversicherung.

- Ausbau der Videoüberwachung:

  Die Implementierung von Videoüberwachung in öffentlich zugänglichen Bereichen privat betriebener Einrichtungen soll erleichtert werden. Das wird vermutlich vor allem öffentliche Veranstaltungen, Einkaufszentren, Diskotheken und andere Orte des öffentlichen Lebens betreffen.

- Scoring und algorithmische Entscheidungen:

  Versicherungen und Krankenkassen soll durch eine Ausnahme in der DSGVO ermöglicht werden Leistungsentscheidungen zukünftig vollautomatisiert zu treffen. Statt dem Prinzip, dass jeder Einzelfall von Menschen zu prüfen ist, soll nun eine algorithmische Auswertung von Gesundheitsdaten und die darauf basierende Entscheidungsfindung von Computern übernommen werden.

- Verarbeitung besonders geschützter Datenkategorien:

  Mit der DSVGO sollen noch mehr Ausnahmen eingeführt werden, die es erlauben besonders sensible Daten zu verarbeiten.

- Einschränkung von Betroffenenrechten:

  Die DSGVO lässt hier eigentlich keine Spielräume für nationale Gesetze zu, dennoch sollten zunächst garantierte Rechte der informationellen Selbstbestimmung heftig beschnitten werden. Geplant

war es, Unternehmen die Lösch- und Auskunftsanfragen von Betroffenen mit der Begründung eines "unverhältnismäßigen Aufwands" ablehnen zu können. Aufgrund massiver Kritik wurden hier Änderungen vorgenommen, die die Einschränkung der Betroffenenrechte auf ein Minimum reduzieren.

Die Große Koalition hat mit dem neuen Datenschutzgesetz neue Rechtsunsicherheiten geschaffen, drängende Fragen nicht geklärt und Potenzial für einen progressiven Grundrechtsschutz verschenkt. Das Gesetz wurde zwar aufgrund heftiger Kritik an wenigen Stellen nachgebessert, blieb aber an den meisten Stellen dennoch unverändert. In einem Interview von netzpolitik.org geht der Datenschutzrechtler Alexander Roßnagel von der Universität Kassel auf die vielen nicht ergriffenen Chancen im neuen Gesetz ein. [17] So werden vom DSGVO viele Herausforderungen der Digitalisierung gar nicht erst thematisiert. In der Verordnung findet sich beispielsweise kein Wort über Big Data, Künstlicher Intelligenz, Smart Cars, Smart Health oder Industrie 4.0.

Für den Bereich des Beschäftigtendatenschutzes und für den öffentlichen Bereich, also für die Datenverarbeitung durch staatliche Stellen und auch durch alle Privaten, die öffentliche Interessen verfolgen, enthält die DSGVO zwei große Öffnungsklauseln. Dieser Bereich macht fast die Hälfte der gesamten Datenverarbeitung aus und hätte durch bereichsspezifische und technikspezifische Regelungen eine Vorbildwirkung für den privaten Bereich. Es hätte auch der EU-Kommission schon einmal wichtige Anhaltspunkte für eine zukünftige Überarbeitung der DSGVO geben können. Stattdessen blieb jedoch eine Ausgestaltung dieser Öffnungsklauseln aus. Auch in anderen Bereichen wurden Öffnungsklauseln nicht weiter ausgestaltet und somit neue Rechtsunsicherheiten geschaffen. So ist zum Beispiel das Privacy-by-Design Prinzip in der DSGVO enthalten, allerdings nur mit einer höchst abstrakten Generalklausel und ohne weitere Spezifikationen. Dieser Grundsatz hängt somit von der freiwilligen Auslegung der Datenverarbeiter ab. Die Hersteller von Datenverarbeitungsprogrammen wurden nicht einmal adressiert in der Klausel. Des Weiteren wurde versäumt klare Ausnahmen für die Nutzung personenbezogener Daten im Rahmen von Presseberichterstattung einzubauen und so möglichen Versuchen vorzubeugen, den Datenschutz zur Einschränkung der Meinungsfreiheit zu instrumentalisieren. Im alten Bundesdatenschutzgesetz fand sich für dieses Problem ein Paragraph, welcher jedoch in der DSGVO ersatzlos wegfällt. Es gibt im DSGVO sogar einen Artikel, der die Datenschutz-Zertifizierung regelt. Hier hätte ein Grundstein für Zertifikate und Siegel gesetzt werden können, jedoch findet sich auch hier nichts Konkretes. Zu den Anforderungen an die Durchführung eines Zertifizierungsprozesses gibt es keine Regeln. Auch hier wird am Ende dem Markt überlassen, wie man die Zertifizierung ausgestaltet. So ist es gut möglich, dass es am Ende schon reicht einfach ein Konzept vorzulegen und eine Papierprüfung vorzunehmen, um ein Datenschutz-Siegel zu erhalten. Die Zertifikate und Siegel würden somit keinerlei Wert besitzen. Das Ziel, mit ihnen das Nutzervertrauen in Internetdienste zu erhöhen wäre somit gescheitert.

Das neue Datenschutzsgesetz hätte die DSGVO also problemlos mit eigenen Paragraphen anpassen können und den Weg zu einem verbesserten und progressiveren Datenschutz ebnen können. Stattdessen wurden Konkretisierungen von der Regierung versäumt, wodurch viele Rechtsunsicherheiten entstanden sind. Die Große Koalition hat jedoch nicht überall auf eigene Paragraphen verzichtet. So wurde die DSGVO im Bereich der Videoüberwachung so drastisch ausgeweitet, dass damit das Risiko eingegangen wird explizit gegen EU-Vorgaben zu verstoßen. In Bereichen wie Privacy-by-Design oder Betroffenenrechte ging, sei es ihnen allerdings zu gefährlich gewesen eigene Gesetzgebungen einzubringen. Das neue Datenschutzgesetz wurde also in Bereichen, in denen es den Datenschutz einschränkt ausgeweitet, sogar mit Risiko gegen EU-Recht zu verstoßen und in den anderen Bereichen so unkonkret wie möglich gelassen.

9 Schluss

Die Privatheit im sozialen Raum hat im Großen und Ganzen sehr gut mit einer Sphärentrennung in öffentlich und privat funktioniert. Dennoch gab es hier natürlich auch Abstufungen. Das Für-sich-Sein in dem das Individuum allein ist. Die Intimität, also das Individuum in einer Liebesbeziehung, mit der Familie oder einer kleinen Gruppe von engen Freunden. Die Anonymität, als die Freiheit in der Öffentlichkeit nicht identifiziert und somit nicht beobachtet zu werden. Und zuletzt die Zurückhaltung, also einfach eine geistige und körperliche Zurückhaltung gegen über anderen Menschen, die sich häufig in Höflichkeitsformeln äußert. Die Privatheit dient hier als Schutz vor Bloßstellung und Manipulation, zum Stress abbauen und zum Finden der inneren Ruhe abseits des Alltags. Sie ist notwendig zur Selbstreflektion und Selbstevaluation des eigenen Verhaltens, indem man beispielsweise den Tag in Ruhe Revue passieren lässt. Darüber hinaus dient die Privatheit im rechtlichen Sinne zur Zuordnung, um Folgen von Handlungen entsprechenden Personen zuweisen zu können.

Der digitale Wandel verkompliziert die Privatheit immens. Auf der einen Seite bringt das Internet neue Jobs, neue Möglichkeiten sich zu vernetzen und unterstützt so die freie Entfaltung, die demokratische Partizipation und das wirtschaftliche Wohlergehen. Auf der anderen Seite bezahlt man für die meisten populären Dienste, wie Facebook und Google, mit seinen persönlichen Daten. Darüber hinaus werden die Spuren, die wir beim Surfen durch das Netz hinterlassen aufgenommen, gesammelt und weiterverarbeitet. Alle diese Daten liegen nun beständig gespeichert auf Servern überall auf der Welt. Im sozialen Raum werden persönliche Informationen Face-to-Face übergeben im Gespräch, natürlich kann auch hier ein drittes Paar Ohren die Konversation mithören, aber das ist einfach zu umgehen. Im Internet bewegen wir uns auf Servern anderer Menschen über Webseiten, die mit Trackern und Analyse-Tools ausgestattet sind. So kann jede unserer Bewegungen mitverfolgt werden. Diese digitalen Spuren und die täglich freiwillig hinterlassenen Informationen im Social Web ergeben riesige Mengen an Daten. Hier spricht man auch von Big Data, denn für die Verarbeitung einer so großen Menge an Daten sind neuere und modernere Analyseprogramme von Nöten. Mithilfe dieser Programme können Daten zusammengeführt, analysiert und verarbeitet werden, dabei entstehen ganz neue Informationen bezüglich der Nutzer. Genutzt werden diese Daten vor allem für personalisierte Werbeanzeigen und sie werden zur Profilbildung verkauft. Viele Datenschützer sehen im Tracking und Scoring von Nutzern schwere Privatsphäreverletzungen. So wird nämlich ein digitales Ich des Nutzers erstellt, dessen Eigenschaften von Algorithmen bestimmt wurde. Diese Eigenschaften werden dann genutzt, um zukünftige Aktionen der realen Person vorherzusehen und auf dieser Basis beispielsweise die Kreditwürdigkeit der Person einzuschätzen oder sie als Arbeitgeber für einen Job zu prüfen. Diese Algorithmen sind allerdings nicht in der Lage die moralischen Ansichten und Intentionen einer Person in irgendeiner Weise zu erfassen und basieren eben nur darauf, wie sich diese Person durch das Internet bewegt. Ein digitales Ich als Bewertungsgrundlage für eine reale Person zu verwenden ist daher sehr fraglich.

Es bedarf also eine Überarbeitung der Privatheit und des Datenschutzes, um mit diesen neuen Gefahren umgehen zu können. Dabei ist es von oberster Priorität, dass die Privatheit und der Datenschutz so ausgestaltet werden, dass sie die Potenziale des Internets nicht einschränken. Am wichtigsten ist hier die Bildung der Menschen in Bezug auf die Nutzung des Internets. Nutzungskompetenzen müssen besser vermittelt werden und der Zugang zu dieser Bildung muss breiter angelegt sein. Der Datenschutz muss so gestaltet werden, dass die Privatheit garantiert ist, er aber nicht mit wichtigen Werten kollidiert. Darüber hinaus ist es wichtig die Vertrauenswürdigkeit der Nutzer in die angebotenen Dienste zu verbessern.

Für die Umsetzung einer solchen angemessenen Privatheit braucht es neben Bemühungen in der Bildung auch welche in Recht, Wirtschaft und Technik. Ohne Anstrengungen in jeden dieser Bereiche gestaltet sich die Umsetzung nur schwer. Die Bildung vermittelt die Nutzungskompetenzen und das Recht sorgt für die gesetzlichen Grundlagen. Die Wirtschaft muss sich der Privatheit verpflichten und sich dem Privacy by Design Prinzip annehmen. Mithilfe von Recht und Technik können Zertifikate und Siegel etabliert werden, welche den Privatheitsschutz der Dienste bewerten. So kann der Schutz der Privatheit anhand der Zertifikate und Siegel verglichen werden und somit zu einem Wettbewerbsvorteil gemacht werden. Die Zertifikate und Siegel sollten dafür unabhängig entwickelt und regelmäßig verbessert und überarbeitet werden. Weiterhin kann die Technik dafür sorgen bessere Grundlagen für den Privatheitsschutz zu schaffen. Vor allem bessere Gestaltungsmöglichkeiten oder neue Datenschutzmethoden, beispielsweise in der Kryptographie, sind für die Nutzer von Vorteil und ermöglicht ihnen einen einfacheren Zugang zum Privatheitsschutz.

Letztendlich muss man auch die Privatsphäre neu denken. Mit dem Aufkommen der sozialen Netzwerke wird das private Leben online zur Schau gestellt. Viele vergessen, dass die Daten nicht nur von Freunden eingesehen werden können, sondern auch beispielsweise der Chef ein Blick aufs Profil werfen kann. Dies kann Auswirkungen auf die berufliche Laufbahn haben, denn nicht alles was man mit seinen Freunden zu bereden hat, würde man auch seinem Chef mitteilen. Menschen stehen zueinander in unterschiedlichen Beziehungen und verhalten sich so je nach Kontext unterschiedlich. Der Arzt kennt Informationen, die man seinen Freunden eventuell nicht erzählt und die Freunde wissen über Aktionen Bescheid, die der Vorgesetzte besser nicht erfahren sollte. Das Konzept der Privatsphäre im Kontext versucht dieses Problem in die Online-Welt zu übertragen und bietet so einen interessanten und neuen Lösungsvorschlag für den Umgang mit der Kommunikation im Netz.

Schlussendlich sollte das Thema Privatheit und Datenschutz wieder verstärkt in den öffentlichen Diskurs gerückt werden. Die vielen neuen Gesetze, wie der Staatstrojaner und das Netzwerkdurchsetzungsgesetz, die aus Sicht des Datenschutzes äußerst fragwürdig haben keine Empörung oder große öffentliche Debatte ausgelöst. Das Thema scheint unter den Teppich gekehrt, die Gefahren sind vielleicht nicht sichtbar genug. Ein Wille zu einer Kultur der Privatheit in Bildung, Recht, Wirtschaft und Technik muss also auch von der Politik selber ausgehen. Es sieht zur Zeit nicht danach aus, mir scheint mit Thomas de Maizière

ist hier eher das Gegenteil der Fall. Dazu kommt die ständige Bedrohung durch den internationalen Terrorismus sowie eine zunehmende politische Spaltung in der Bevölkerung mit dem Erstarken der Alternative für Deutschland. Dennoch wäre eine neue Privatheitskultur und die Annahme von Konzepten wie der Privatsphäre im Kontext zielführend für einen neuen und besseren Schutz der Privatheit und der Daten.

Literatur

[1] "Der Soziale Raum."
http://www.student-online.net/Publikationen/150/original_154_student_online.html.
Abgerufen am 31. Juli 2017.

[2] A. F. Westin, "Privacy and freedom," *Atheneum. New York*, 1967.

[3] S. Krämer, "Verschwindet der Körper? Ein Kommentar zu virtuellen Räumen," in *Wissen Raum Macht*, pp. 60–63, Maresch, Rudolf and Werber, Nils, 2002.

[4] klicksafe.de. EU-Initiative für mehr Sicherheit im Netz, "Privatsphäre und Big Data."
http://www.klicksafe.de/themen/medienethik/privatsphaere-und-big-data/.
Abgerufen am 7. August 2017.

[5] "Informationssicherheit. Secupedia.."
http://www.secupedia.info/wiki/Informationssicherheit.
Abgerufen am 9. August 2017.

[6] "Datensicherheit. Secupedia.."
http://www.secupedia.info/wiki/Datensicherheit.
Abgerufen am 9. August 2017.

[7] "Informationsschutz. Secupedia."
http://www.secupedia.info/wiki/Informationsschutz.
Abgerufen am 9. August 2017.

[8] T. Weichert, "Datenschutzverstoß als Geschäftsmodell - der Fall Facebook," *Datenschutz und Datensicherheit-DuD*, vol. 36, no. 10, pp. 716–721, 2012.

[9] acatech, "Privatheit im Internet. Chancen wahrnehmen, Risiken einschätzen, Vertrauen gestalten. (acatech POSITION)," Heidelberg u.a.: Springer Verlag, 2013.

[10] H. Nissenbaum, "Privatsphäre im Kontext: Technologie, Politik und die Unversehrtheit des Sozialen," *Heinrich Böll Stiftung: Schriften zu Bildung und Kultur*, vol. 8, pp. 53–63, 2011.

[11] P. D. J. Limbach, "Ist die kollektive Sicherheit Feind der individuellen Freiheit? Zeit Online.."
http://www.zeit.de/reden/deutsche_innenpolitik/200221_limbach_sicherheit, 2013.
Abgerufen am 6. September 2017.

[12] "Minister de Maizière für flächendeckende biometrische Videoüberwachung. netzpolitik.org.."
https://netzpolitik.org/2017/minister-de-maiziere-fuer-flaechendeckende-biometrische-videoueberwachung/.
Abgerufen am 7. September 2017.

[13] "Bundestag will weitreichendes Überwachungsgesetz beschließen. Süddeutsche Zeitung.."
http://www.sueddeutsche.de/digital/staatstrojaner-bundestag-will-weitreichendes-ueberwachungsgesetz-beschliessen-1.3554426.
Abgerufen am 7. September 2017.

[14] "Hate-Speech-Gesetz: Neuer Entwurf gefährdet weiterhin die Meinungsfreiheit. netzpolitik.org.."
https://netzpolitik.org/2017/hate-speech-gesetz-neuer-entwurf-gefaehrdet-weiterhin-die-meinungsfreiheit/.
Abgerufen am 7. September 2017.

[15] "Verstoss gegen EU-Recht: Bundestag verabschiedet NetzDG."
https://digitalegesellschaft.de/2017/06/netzdg-verabschiedet/.
Abgerufen am 7. September 2017.

[16] "Was lange währt, wird endlich ... immer noch nicht gut. Die Kritik am neuen Datenschutzgesetz im Überblick. netzpolitik.org."
https://netzpolitik.org/2017/was-lange-waehrt-wird-endlich-immer-noch-nicht-gut-die-kritik-am-neuen-datenschutzgesetz-im-ueberblick/.
Abgerufen am 7. September 2017.

[17] “”Chance verpasst”: Interview zum neuen Datenschutzgesetz. netzpolitik.org.”
https://netzpolitik.org/2017/chance-verpasst-interview-zum-neuen-datenschutzgesetz/.
Abgerufen am 7. September 2017.