



universität
wien

MAGISTERARBEIT

Titel der Magisterarbeit

Der Spion in der Hosentasche

Eine qualitative Untersuchung über das Wissen von jungen
Erwachsenen im Hinblick auf Big Data und der Smartphone-Nutzung

Verfasserin

Barbara Mayr

Angestrebter akademischer Grad

Magistra der Philosophie (Mag. phil.)

Wien, 2015

Studienkennzahl lt. Studienblatt:

Studienrichtung lt. Studienblatt:

Betreuerin:

A 066 841

Magisterstudium

Publizistik- und Kommunikationswissenschaft

Ass.-Prof. Mag. Dr. Gerit Götzenbrucker, Privatdoz.

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Wien, April 2015

Barbara Mayr

Danksagung

Mein erster und größter Dank geht an meine Eltern, die mir dieses Studium ermöglicht haben und auf deren Unterstützung und Vertrauen ich mich immer verlassen konnte. Sie waren oft gute Zuhörer und Ratgeber. Von Herzen danken möchte ich auch meinem Partner Alexander, der mich durch die Höhen und Tiefen dieses Studiums begleitet hat, mir stets Hoffnung und Zuversicht schenkte und bei dem ich immer Ruhe und Kraft gefunden habe.

Ein herzliches Dankeschön möchte ich meinen Freunden aussprechen, die mir im Zuge dieser Magisterarbeit gute Ratschläge und Motivation schenkten.

Ein aufrichtiges Danke für die gesamte Betreuung und die motivierenden Denkanstöße geht an Frau PD Ass.-Prof. Dr. Gerit Götzenbrucker, welche sich immer um meine Anliegen gekümmert hat.

Ein besonderer Dank auch an alle UntersuchungsteilnehmerInnen, die sich die Zeit für diese Untersuchung genommen haben und die Fragen gewissenhaft beantworteten. Ohne sie wäre der empirische Teil nicht in dieser Form zustande gekommen.

Inhaltsverzeichnis

1. Einleitung.....	11
1.1. Zugrundeliegendes Problem.....	12
1.2. Erkenntnisinteresse.....	13
1.3. Aufbau der Arbeit.....	13
2. Aktuelle Forschungsergebnisse	15
3. Grundlegende kommunikationswissenschaftliche Theorie	22
3.1. Konstruktivismus	22
3.2. Konstruktivistische Medientheorie	23
3.3. Kommunikativer Konstruktivismus	24
4. Das Konstrukt Wissen	25
4.1. Die Vermittlung von Wissen in der Gesellschaft.....	25
4.2. Die Entwicklung von Daten, über Informationen, hin zu Wissen	25
4.3. Die Dimensionen des Wissens	26
4.4. Die Wissensarten.....	27
5. Big Data.....	28
5.1. Begriffsdefinition	28
5.2. Was ist Big Data?	29
5.3. Woher kommen die Daten?.....	31
5.4. Möglichkeiten, Risiken und Folgen von Big Data.....	32
6. Daten.....	36
6.1. Der Datenschutz – eine Reaktion auf technische Neuerungen	36
6.1.1. Begriffsdefinition.....	36
6.1.2. Datenschutz in Österreich	37
6.1.3. Datenschutz in Deutschland.....	37
6.1.4. Datenschutz in Italien	38
6.1.5. Datenschutz in der EU	38
6.1.6. Datenschutzabkommen zwischen Europa und den USA.....	39
6.1.7. Das Verhältnis von Big Data und Datenschutz.....	39
6.2. Die Datensicherheit	40

6.3.	Die Berührungspunkte von Datenschutz und Datensicherheit.....	41
6.4.	Begriffsdefinition: Daten im Sinne des Datenschutzes.....	41
6.5.	Die Verwendung von Daten.....	42
6.6.	Die Vorratsdatenspeicherung	43
6.7.	Die Überwachung der Telekommunikation heute	43
6.8.	Der Datenschutz am eigenen Smartphone	44
7.	Das Post-Privacy- Zeitalter.....	45
7.1.	Begriffsdefinition	45
7.2.	Die Möglichkeiten des Data Mining	45
7.3.	Machtverhältnis – Der Kontrollverlust unserer Daten	46
7.4.	Vor- und Nachteile eines Lebens ohne Privatsphäre	46
7.5.	Die Transparenzgesellschaft als Folge der heutigen Informationstechnik.....	47
8.	Forschungsfragen.....	49
9.	Untersuchung.....	50
9.1.	Forschungsdesign	50
9.2.	Untersuchungsgegenstand.....	51
9.3.	Untersuchungsmaterial.....	52
9.4.	Transkription	52
9.5.	Untersuchungsmethode	53
9.5.1.	Leitfadeninterview – Vorteile und Kritik	53
9.5.1.1.	Interviewfragen.....	54
9.5.2.	Qualitative Inhaltsanalyse – Vorteile und Kritik	54
9.6.	Kategoriensystem	55
10.	Auswertung	56
10.1.	Kategorie 1: Medienkonsum	56
10.2.	Kategorie 2: Smartphonegebrauch	57
10.3.	Kategorie 3: Wissen über Big Data	58
10.4.	Kategorie 4: Datenschutz.....	58
10.5.	Kategorie 5: Datenspeicherung und Datenzugriff	68
10.6.	Kategorie 6: Datenanalyse.....	71
10.7.	Kategorie 7: Mögliche Folgen von Big Data.....	72
11.	Beantwortung der Forschungsfragen	78
12.	Interpretation und Diskussion der Forschungsergebnisse.....	80

13.	Ausblick	86
14.	Limitationen der Forschung	86
15.	Quellenverzeichnis	88
15.1.	Literaturverzeichnis:	88
15.2.	Internetverzeichnis:	90
16.	Anhang	95
16.1.	Interviewleitfaden:	95
16.2.	Transkriptionsregeln:	99
16.3.	Transkribierte Interviews	99
16.4.	Beispiel Kategoriensystem	238
	Abstract - deutsch	256
	Abstract - english	257
	Curriculum Vitae	258

1. Einleitung

Es beginnt schon früh morgens, sobald unser Handywecker klingelt, und setzt sich beim Frühstück oder auf dem Weg zur Arbeit fort: die mittlerweile sehr intensive Nutzung eines Smartphones in jeder möglichen Lebenslage. Mit der Wetter-App bestimmen wir das Outfit für den Tag, die Aktualisierung des E-Mailordners hält uns auf dem Laufenden und anschließend informieren wir uns noch via Facebook und auf Online-Nachrichtenseiten was in unserem Freundeskreis und im Weltgeschehen so passiert.¹ Smartphones sind persönliche Geräte, die uns im Alltag permanent begleiten und das in einem weit größerem Ausmaß als andere Geräte der Informations- und Kommunikationstechnik.² „Neben Hausschlüssel und Geldbeutel gehört das Smartphone für viele Nutzer mittlerweile zur täglichen Grundausstattung“³, schreibt die Zeitung *Horizont* im Juni 2013. Daran hat sich bis heute nichts geändert.

Neben dem Telefonieren bieten verschiedene installierbare Programme (Apps), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die, durch deren Nutzung, entstandenen Daten lassen anschließend detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.⁴ Anders als bei herkömmlichen Computern ermöglichen Smartphones den Nutzern die Kontrolle oder Vermeidung von Datenpreisgabe nur in einem sehr geringen Umfang.⁵ „Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt.“⁶ Die Zeitschrift *Datenschutz und Datensicherheit* spricht daher berechtigt von einem „Spion in der Hosentasche“⁷. Die Kombination an Unmengen von gespeicherten Daten über uns und den neuen Technologien, die es ermöglichen diese Daten zu analysieren und auszuwerten, können für uns Vorteile, aber auch Gefahren und Risiken mit sich bringen.

¹ Siehe auch: Nemitz, Gordon; Rieder, Christian (2011): Homo Smartphone. GDI Impuls, 2. S. 88. Abrufbar unter: http://www.wiso-net.de/webcgi?START=A20&T_FORMAT=5&DOKM=1881856_ZECO_0&TREFFER_NR=1&WID=67322-7360574-81226_10 (16.05.2014)

² Vgl. Datenschutz und Datensicherheit (06/2011): Datenschutzgerechte Smartphone-Nutzung ermöglichen! Datenschutz und Datensicherheit – DuD, 35 (6). S. 386. Abrufbar unter: <http://link.springer.com/article/10.1007%2Fs11623-011-0095-x> (16.05.2014)

³ Lang, Katrin (27.06.2013): User tauschen sich gerne aus. Seven-One prüft mit Mobile Barometer Smartphone-Nutzung. *Horizont* 26. S. 7. Abrufbar unter: http://www.wiso-net.de/webcgi?START=A40&OVVAR=DOK_SPEICHERN,EINZEL_DOK,EINZEL_TITEL,PDF_ALLO_W,RTF_ALLOW&DOK_SPEICHERN=1&EINZEL_DOK=2449691_ZECO_0&EINZEL_TITEL=Seven_One_Media_Inter&PDF_ALLOW=1&RTF_ALLOW=1&WID=67322-7360574-81226_2 (16.05.2014)

⁴ Vgl. Datenschutz und Datensicherheit (06/2011). S. 386

⁵ Vgl. Datenschutz und Datensicherheit (06/2011). S. 386

⁶ Datenschutz und Datensicherheit (06/2011). S. 386

⁷ Datenschutz und Datensicherheit (06/2011). S. 386

1.1. Zugrundeliegendes Problem

Alle Bewegungen, die wir im Internet machen, werden als Daten gespeichert. Dabei spielt es keine Rolle von welchem mobilen Endgerät aus das Internet genutzt wird. Da mittlerweile sehr viele Geräte um uns herum mit dem Internet verbunden sind, produzieren wir ununterbrochen Daten, sodass Kommunikationsexperten von einer Datenlawine mit tsunamiartigen Ausmaß sprechen.⁸ Aus den Unmengen an gespeicherten Daten hinterlassen wir eine digitale Spur im Internet, und das bei jeder Benützung. Je öfter wir online sind, umso größer und umfangreicher wird unsere persönliche digitale Spur. Laut IBM produzieren wir heute pro Tag Daten im Ausmaß von 2,5 Quintillionen Bytes. Die Tendenz steigt, denn 90% der heutigen Internetdaten sind in den letzten drei Jahren entstanden.⁹ „Weltweit steigt die Datenmenge so rasend schnell, dass sie nicht nur die Verarbeitungskapazität der Rechner, sondern auch unser Vorstellungsvermögen übersteigt.“¹⁰ Mit Hilfe der neuen Technologien gelingt es Unternehmen die großen Datensätze zu ordnen und zu analysieren. Algorithmen helfen dabei unsere Daten auszuwerten und ermöglichen eine vorausschauende Datenanalyse, welche aus den Daten unserer Vergangenheit unser Verhalten in der Zukunft vorhersagen kann. Laut den Big Data-Mathematikern ist unser Verhalten nämlich nicht zufällig, sondern folgt eindeutigen Gesetzen. Big Data verkörpert diese Möglichkeit, aus scheinbar unnützen Datensätzen, wertvolle Informationen für Personen, Wirtschaft und unsere Welt zu eruieren. Big Data bringt viele Möglichkeiten mit sich, welche unser Leben verbessern können, immer jedoch mit der Kombination von Risiken und Gefahren, vor denen wir uns schützen sollten. Es spielt eine entscheidende Rolle, ob Menschen über Big Data und seine Möglichkeiten und Gefahren Bescheid wissen und infolge dessen bewusst mit der Bereitstellung der eigenen Daten umgehen, oder ob sie persönliche, sensible Daten ahnungslos und oft ungewollt veröffentlichen. Datenschutz ist ein zentrales Thema der Big Data-Debatte. Der Online-Datenschutz wird durch das Wissen der Personen maßgeblich beeinflusst: Wissen über Datenschutz geht signifikant mit einem besseren

⁸ Vgl. Klausnitzer, Rudi (2013): Das Ende des Zufalls. Wie Big Data uns und unser Leben vorhersagbar macht. 1. Auflage. Salzburg: Ecowin Verlag. S. 9

⁹ Vgl. Knapp, Moureen „Molly“ (21.11.2013): Big Data. Journal of Electronic Resources in Medical Libraries. 10 (4). S.215-222. Abrufbar unter: <http://www.tandfonline.com/doi/abs/10.1080/15424065.2013.847713#.U01WDKJqzeo> (16.05.2014)

¹⁰ Mayer-Schönberger, Viktor; Cukier, Kenneth (2013): Big Data. Die Revolution, die unser Leben verändern wird. 1. Auflage. München: Redline Verlag. S. 15

Schutz der Daten einher, sei es in sozialer, als in technischer Dimension¹¹. Ein mangelndes Wissen über Big Data und dessen Folgen, kann fatale Folgen für die Konsumenten nach sich ziehen.

1.2. Erkenntnisinteresse

Das Erkenntnisinteresse dieser Arbeit ergibt sich aus dem zugrundeliegenden Problem. Es fragt nach dem Wissen der Konsumenten im Alter zwischen 18 und 24 Jahren über die Speicherung und Analyse ihrer Daten. Da Big Data jegliche Art von Daten speichert und zur Analyse verwendet, sind bei der Frage sowohl freiwillig, als auch unfreiwillig dargebotene Daten, sowie bewusste, wie unbewusst erzeugte Daten gemeint. Eine sich anschließende Frage lautet, wie viel diese Personen über das Ziel bzw. den dahinterstehenden Gedanken und die möglichen Folgen von Big Data wissen. Einen besonderen Fokus legt die Untersuchung auf die Nutzung von Smartphones. Zum einen, weil uns unser Smartphone beinahe 24 Stunden auf Schritt und Tritt begleitet, zum anderen, weil laut der 2014 erschienenen U25-Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVISI), junge Menschen überwiegend durch das Smartphone mit dem Internet verbunden sind.¹²

1.3. Aufbau der Arbeit

Die vorliegende Arbeit wird in einen theoretischen und empirischen Teil gegliedert. Im ersten, theoretischen Teil wird Bezug genommen auf die aktuellen Forschungsergebnisse zum Thema Datenschutz und Preisgabe von Daten in Verbindung mit dem eigenen Wissenstand. Leider finden sich zwar unzählige Studien zu diesen einzelnen Themen, eine Kombination von persönlichem Wissen und Datenschutz, sowie Privatsphäre untersuchen hingegen nur einzelne Studien. Um einen allgemeinen Überblick über den Smartphonegebrauch und dem damit einhergehenden Datenschutz und der Privatsphäre zu geben, werden auch weitere Studien in diesem Bereich beachtet. Anschließend wird auf die grundlegende Theorie des Konstruktivismus aus kommunikationswissenschaftlicher Sicht kurz eingegangen und der Kommunikative

¹¹ Vgl. Yong, Jin Park; Scott, W. Campbell; Nojin, Kwak (06/2012): Affect, cognition and reward: Predictors of privacy protection online. Computers in Human Behavior. 28 (3). S. 1024. Abrufbar unter: <http://www.sciencedirect.com/science/article/pii/S0747563212000064> (03.07.2014)

¹² Vgl. DIVISI (02/2014): U25-Studie. Kinder, Jugendliche und junge Erwachsene in der digitalen Welt. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVISI). Hamburg. S. 12

Konstruktivismus skizziert. Das Konstrukt Wissen wird in einem eigenen Kapitel erörtert. Eingegangen wird dabei vor allem auf die Vermittlung von Wissen in sozialen Gesellschaften und die Entwicklung von Daten über Informationen, hin zu Wissen. Die einzelnen Wissensdimensionen und Wissensarten geben Aufschluss darüber, wie sich das Wissen theoretisch zusammensetzt und in welcher Form es abrufbar und explizierbar ist und somit untersucht werden kann. Im fünften Kapitel wird Big Data diskutiert. Eingeleitet mit einer Begriffsdefinition wird erklärt was man sich unter Big Data vorstellen kann und woher die Daten für die Speicherung und anschließenden Analysen stammen. Es wird ein Überblick gegeben, welche Möglichkeiten ExpertInnen in Big Data sehen, diese werden gegenübergestellt und diskutiert, und es wird aufgezeigt welche Risiken und Folgen Big Data für uns haben kann. Da Big Data bereits gespeicherte Daten zum Teil auch für aktuelle Analysen wiederverwendet, wird das Verhältnis zum Datenschutz diskutiert. Die unterschiedliche Verwendung von Daten hat einen wesentlichen Einfluss auf die Entwicklungen hinsichtlich Big Data. Der Datenschutz wird als Reaktion auf die technischen Neuerungen erklärt und in Österreich, Deutschland, Italien und der EU skizziert. Angesprochen, durch den massiven Transfer von Daten europäischer Bürger in amerikanische Unternehmen, wird ebenso das Datenschutzabkommen zwischen Europa und den USA. Da Datenschutz und Datensicherheit häufig in einem Atemzug genannt werden, wird auch auf ihre Unterschiede, sowie Berührungspunkte Bezug genommen. Es wird ein Einblick gegeben, welches Ausmaß die Überwachung der Telekommunikation bereits angenommen hat und wieso die Vorratsdatenspeicherung derzeit außer Kraft ist. Die Autorin hält es für notwendig nach der Auflistung aller Risiken und möglichen Folgen auch Hinweise für einen angemessenen Datenschutz am eigenen Smartphone zu geben und somit aufzuzeigen, welche Möglichkeiten es für die Konsumenten gibt, sich so gut wie möglich zu schützen.

Welche Folgen, Vor- und Nachteile Experten durch eine in allen Bereichen geforderten Transparenz vermuten, wird im Kapitel sieben erklärt. Angesprochen wird dabei auch der Kontrollverlust unserer Daten, welcher das Machtverhältnis in unserer Gesellschaft neu definiert. Mit dem Data Mining wird es sogar ermöglicht Informationen zu generieren, die niemals preisgegeben wurden.

Mit den Forschungsfragen wird der zweite, empirische Teil eröffnet und die Untersuchung geleitet. Das Forschungsdesign, der Untersuchungsgegenstand und – material, die Transkription und die Untersuchungsmethoden geben Aufschluss über die

Forschung und Durchführung. Das Kategoriensystem erklärt mit welchem Suchraster die Interviews ausgewertet wurden. Die anschließende Auswertung ist sehr detailliert verfasst und vermittelt einen umfassenden Überblick über den Wissenstand der Untersuchungspersonen. Im Anschluss an die Auswertung werden die Forschungsfragen beantwortet und die Ergebnisse interpretiert und im Bereich des aktuellen Forschungsstandes diskutiert.

Im Ausblick werden Möglichkeiten für anschließende Forschungen gegeben und die Limitationen, welchen die Forschung erlag, erklärt.

2. Aktuelle Forschungsergebnisse

Eine umfangreiche Studie zum Thema *Kinder, Jugendliche und junge Erwachsene in der digitalen Welt* veröffentlichte das DIVISI im Februar 2014. Die Ergebnisse zeigen die Wichtigkeit des Internets für junge Erwachsene und insbesondere dessen Nutzung auf dem Smartphone auf. „Online sein zu können, stellt für junge Menschen ein zentrales Element der gesellschaftlichen Teilhabe dar.“¹³ Dabei nutzen 72 Prozent der 18 bis 24 Jährigen das Internet täglich, 22 Prozent mehrmals pro Woche und nur drei bzw. zwei Prozent selten bzw. nie.¹⁴ Die „72 Prozent [...], die das Internet täglich nutzen, verwenden dazu ihr Smartphone oder ihr Handy“¹⁵, wobei der wichtigste Aspekt der Internet-Nutzung die Kommunikation mit Freunden ist.¹⁶

Welche Rolle Apps dabei spielen, berichtet die JIM 2014 – Jugend, Information, (Multimedia) Media. Messenger Apps zählen für 86 Prozent der 12 bis 19-Jährigen zu den wichtigsten Apps. WhatsApp haben 94 Prozent der Besitzer von internetfähigen Handys installiert.¹⁷ Die Kommunikation via SMS wurde von den Messenger-Apps zum Großteil übernommen. Während 2013 noch 72 Prozent via SMS kommunizierten, tun dies 2014 nur mehr 45 Prozent.¹⁸ Community-Apps folgen mit Abstand den Messenger-Apps mit 46 Prozent, wobei es sich hier vor allem um die Facebook-App handelt (43%).¹⁹

¹³ DIVISI U-25-Studie, 2014. S. 11

¹⁴ Vgl. DIVISI U-25-Studie, 2014. S. 62

¹⁵ DIVISI U-25-Studie, 2014. S. 65

¹⁶ Vgl. DIVISI U-25-Studie, 2014. S. 61

¹⁷ Vgl. JIM-Studie 2014, Medienpädagogischer Forschungsverbund Südwest (11/2014): JIM 2014 Jugend, Information (Multimedia) Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Stuttgart. S. 49-50 Abrufbar unter: http://www.mpfs.de/fileadmin/JIM-pdf14/JIM-Studie_2014.pdf (10.01.2015)

¹⁸ Vgl. JIM, 2014. S. 47

¹⁹ Vgl. JIM, 2014. S. 49

Eine Folge dieses mobilen Online-Seins ist das subjektive Empfinden der jungen Erwachsenen ständig online zu sein.²⁰ Damit geht ein neues Verständnis von Privatsphäre einher. „Der Umgang mit den eigenen privaten Informationen wird (...) zu einer kontinuierlichen, pragmatischen Kosten-Nutzen-Abwägung. (...) Zu wissen, wann welche Information für wen relevant ist, gilt als Kernkompetenz im Online-Verhalten.“²¹ Online wird dabei ein Maß an Privatheit angestrebt, das es ermöglichen soll, zu wissen, was andere von einem wissen, effektiv zu verbreiten, was andere von einem selbst wissen sollten und zusätzlich soll gewährleistet sein, an die persönlich relevanten Informationen von wichtigen Kontakten zu gelangen.²²

93 Prozent der befragten 18- bis 24-jährigen Facebook-Nutzer besprechen daher sehr private Themen auch lieber persönlich unter vier Augen, als online in Communitys, sind aber der Meinung, dass man in einer Online-Community Daten über sich preisgeben soll (45%), da es bei einem guten Schutz der persönlichen Daten aller langweilig in diesen Communitys wäre (37%).²³ Die Studie zeigt, dass die Verletzung der Privatsphäre für junge Erwachsene unterdurchschnittlich relevant ist, dafür aber die kriminellen Übergriffe für sie eine überdurchschnittlich große Rolle spielen.²⁴

Interessant in Hinblick auf dieses Forschungsvorhaben sind die Ergebnisse der Befragung zum Thema *Risikowahrnehmung* bei der Internet-Nutzung.²⁵ Die Studie fragt nach den einzelnen Risiken und ob sie auch tatsächlich schon erlebt wurden. Im Alter zwischen 18 und 24 Jahren sehen 55 Prozent der Befragten die unerwünschte Weitergabe von persönlichen Daten an Dritte als Risiko an, wobei jedoch nur 9 Prozent auch angeben, dass sie davon bereits betroffen waren.

Ähnlich verhält es sich mit der Spionage persönlicher Daten: 53 Prozent sehen es als Risiko der Internetnutzung, aber nur 3 Prozent geben an, dass ihnen das bereits passiert ist. Bei der Nutzung persönlicher Daten für Werbezwecke verhält sich das Risikobewusstsein mit dem Bewusstsein, dass dies bereits geschehen ist mit 38 Prozent zu 13 Prozent. Ein anderes Ergebnis zeigt sich beim Ausspionieren der Zugangsdaten zum Online-Banking mit 33 Prozent zu ein Prozent. Die Veröffentlichung peinlicher/intimer Chats oder Posts sehen 27 Prozent gefährlich, sechs Prozent berichten

²⁰ Vgl. DIVISI U-25-Studie, 2014. S. 68

²¹ DIVISI U-25-Studie, 2014. S. 116

²² Vgl. DIVISI U-25-Studie, 2014. S. 116

²³ Vgl. DIVISI U-25-Studie, 2014. S. 117

²⁴ Vgl. DIVISI U-25-Studie, 2014. S. 150

²⁵ Vgl. Dazu alle Ergebnisse: DIVISI U-25-Studie, 2014. S. 127-129

darüber. Gering befürchten bzw. erlebten die Nutzer den Verlust bzw. die Löschung persönlicher Daten (22 Prozent bzw. zwei Prozent), die Gefahr, dass andere wissen, was man selbst gerade macht bzw. wo man gerade ist (17 Prozent bzw. fünf Prozent), sowie andere Formen von Kriminalität im Internet (16 Prozent bzw. zwei Prozent). Laut dem aktuellen Stand der Forschung zum Thema Big Data, der anschließend behandelt wird, kann hier bei jedem erwähnten Risiko davon ausgegangen werden, dass jeder Nutzer von den Risiken betroffen war, wenn keine spezielle Verschlüsselung der eigenen Internetnutzung verwendet wurde. Da laut dem Telekom-Datenschutzbericht 2013 nur neun Prozent der Internetnutzer in Deutschland eine Verschlüsselungssoftware für E-Mails verwendeten²⁶, kann davon ausgegangen werden, dass die Prozentwerte der Studie nicht aufgrund der möglicherweise verwendeten Verschlüsselungssoftwares zustande kamen. Ausgehend von diesen Ergebnissen wird vermutet, dass das Bewusstsein über Big Data äußerst gering ist.

Bezüglich des Wissens von Gefahren zeigt die Studie (sie untersuchte im Speziellen das Thema Mobbing), dass die hohe Präsenz von Themen in medialen Diskursen sich erkennbar in den Wissensbeständen der jungen Erwachsenen niederschlägt.²⁷ Somit kann auch beim Thema Big Data davon ausgegangen werden, dass bei medialer Berichterstattung die Aufmerksamkeit für dieses Thema steigt.

Auch bei den Ergebnissen im Bereich Sicherheit zeigt sich ein geringes Wissen. Die Studie zeigt auf, dass sich für rund ein Drittel der jungen Erwachsenen durch die Berichterstattungen von Geheimdiensttätigkeiten im digitalen Raum das Sicherheitsgefühl verschlechtert hat, allerdings ohne Konsequenzen für die online investierte Zeit der Nutzer (nur vier Prozent sind bereit ihre Online-Zeit zu reduzieren).²⁸ Das Wissensdefizit wird besonders bei der Frage nach dem Missbrauch von persönlichen Daten deutlich. 19 Prozent der jungen Erwachsenen sind sich sicher, dass ihre persönlichen Daten im Internet noch nicht missbraucht wurden, 41 Prozent stimmen dem eher zu, 24 Prozent stimmen dem eher nicht zu und nur 8 Prozent stimmen dem überhaupt nicht zu.²⁹ Dem entgegen finden sich viele Beweise, dass dem nicht so ist. Laut Michael

²⁶ Vgl. Deutsche Telekom AG (2014): Zahlen, Daten Fakten. Datenschutz und Datensicherheit. Bericht 2013. S. 33. Abrufbar unter: <http://telekom2.de/dud2013/>

²⁷ Vgl. DIVISI U-25-Studie, 2014. S. 130

²⁸ Vgl. DIVISI U-25-Studie, 2014. S. 12, 142

²⁹ Vgl. DIVISI U-25-Studie, 2014. S. 142

Hange, Präsident des Bundesamtes für Sicherheit in der Informationstechnik, registrierte das BSI innerhalb von drei Monaten im Jahr 2013 etwa 250.000 Identitätsdiebstähle.³⁰

Die JIM-Studie 2014 liefert hierzu andere Ergebnisse, die jedoch lediglich das Sicherheitsgefühl widerspiegeln. Auf die Frage wie sicher sich Jugendliche hinsichtlich ihrer Daten in online Communitys fühlen, geben nur sieben Prozent die Antwort „sehr sicher“. 39 Prozent fühlen sich „sicher“, die Mehrheit jedoch (36% bzw. 18%) fühlen sich „weniger sicher“ bis „gar nicht sicher“.³¹

Auf die Wichtigkeit von Wissen über Datenschutz weisen auch Studien wie beispielsweise jene von Yong Jin Park, Scott W. Campbell, Nojin Kwak *Affect, cognition and reward: Predictors of privacy protection online*³² hin. Die Ergebnisse der Studie zeigen auf, dass Wissen eine große Rolle beim Online-Datenschutz spielt und Wissen signifikant mit einem besseren Schutz der Daten, sei es in sozialer, als in technischer Dimension, einhergeht.³³

Aber auch die Ergebnisse der Studie von Kuang-Wen Wu, Huang Shaio Yan, Yen David C., Popova Irina *The effect of online privacy policy on consumers privacy concern and trust* kann auf das Wissen der Konsumenten zurückgeführt werden.³⁴ Sie beweist signifikante Zusammenhänge von Bedenken über Datenschutz und der Bereitschaft persönliche Informationen preiszugeben, sowie dem Vertrauen und der Bereitschaft persönliche Informationen preiszugeben. Die Ergebnisse der Studie zeigen auf, dass für die Nutzer einer Webseite der Inhalt der Datenschutzrichtlinien wichtig ist und auch ihre Nutzung der Webseite beeinflusst, wenn als Voraussetzung für die Nutzung persönliche Informationen angegeben werden müssen.³⁵

Relevante Ergebnisse dazu liefert die JIM 2014. Sie zeigt, dass 80 Prozent der App-Nutzer wissen, dass Apps, egal ob geographische Apps oder andere, Daten vom eigenen

³⁰ Vgl. Bundesamt für Sicherheit in der Informationstechnik (26.09.2013): Kompass zur sicheren Internetnutzung von Polizei und BSI. Stuttgart/Bonn. Abrufbar unter: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Kompass_zur_sicheren_Internetnutzung_26092013.html (07.07.2014)

³¹ Vgl. JIM-Studie 2014. S. 39

³² Vgl. Yong Jin Park et al. 2012. S. 1019-1027.

³³ Vgl. Yong Jin Park et al. 2012. S. 1024

³⁴ Vgl. Wu, Kuang-Wen; Huang, Shaio Yan; Yen, David C.; Popova, Irina (2012): The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*. 28 (3). S. 889-897
Abrufbar unter: <http://www.sciencedirect.com/science/article/pii/S0747563211002767> (03.07.2014)

³⁵ Vgl. Wu et al., 2012. S. 896

Handy auslesen und an die Anbieter weitergeben. 56 Prozent geben an, dass sie die Übertragung von Ortungsdaten generell deaktiviert haben, 17 Prozent haben dies nur für bestimmte Dienste ausgeschaltet. Nur sieben Prozent lassen die Übertragung allgemein zu.³⁶ Im Hinblick auf die Lokalisierungsmöglichkeit mit Hilfe von Ortungsdaten des eigenen Smartphones herrscht bei den jungen Erwachsenen eine recht hohe Sensibilität vor.

Da besonders bei den unter 30-Jährigen ein breites Spektrum an genutzten Anwendungen vorliegt und mindestens 24 Anwendungen regelmäßig von 57 Prozent der unter 30-Jährigen genutzt werden, zeigt die *DIVISI Studie zu Freiheit versus Regulierung im Internet* auf, dass die Risiken, welche durch die Internetnutzung entstehen, den Nutzern dabei bewusst sind.³⁷ Interessant ist, dass sich die Sorgen der einzelnen Untersuchungsgruppen der Studie kaum unterscheiden. Sowohl jüngere, als auch ältere, wie intensive versus seltene Nutzer zeigen nur minimale Unterschiede hinsichtlich der Risikoeinschätzung auf. Die Gefahr, dass der Rechner mit Viren infiziert wird, ist dabei besonders hoch. Aber auch die Befürchtung der Überwachung, des unerlaubten Zugriffs von Personen zu ihrem Computer, sowie des Betrugs und Missbrauchs sind bei mehr als der Hälfte der Internetnutzer vorhanden.³⁸ Bei genauer Nachfrage welche schlechten Erfahrungen bereits gemacht wurden, geben 58 Prozent an, dass ihr Rechner bereits von Viren befallen wurde, immerhin 24 Prozent sagen aus, dass über gefälschte Mails versucht wurde, an persönliche Informationen wie Passwörter und Kontodaten zu kommen. Dass sich andere Personen Zugang zum eigenen Computer verschaffen konnten, war bei vier Prozent der gesamten Internetnutzern der Fall. Auch der Missbrauch von persönlichen Daten, wie Kreditkartennummern oder Bankverbindungen liegt mit drei Prozent gering.³⁹

Insgesamt überwiegt in der bundesdeutschen Bevölkerung aber die Meinung des Vorteils der Internetnutzung. Diese steigt mit der Intensität der Nutzung an⁴⁰, ebenso wie auch das

³⁶ Vgl. JIM-Studie, 2014, S. 51

³⁷ Vgl. DIVISI (12/2013): Studie zu Freiheit versus Regulierung im Internet. Eine repräsentative Bevölkerungsbefragung des Instituts für Demoskopie Allendörfer (IfD) im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVISI), Hamburg, S. 10

³⁸ Vgl. DIVISI Studie, 2013 S. 23f.

³⁹ Vgl. DIVISI Studie, 2013, S. 26

⁴⁰ Vgl. DIVISI Studie, 2013, S. 28

Vertrauen, Risiken gut einschätzen zu können.⁴¹ Allerdings zeigt die Studie auch auf, dass besonders bei der Speicherung und Verwendung von persönlichen Informationen große Unsicherheit herrscht. 26 Prozent der Intensiv-Nutzer geben an, gut einschätzen zu können wofür Suchbegriffe bei Suchmaschinen verwendet werden.⁴² Welche Informationen Suchmaschinen etc. über die eigene Person speichern, können immerhin nur mehr 14 Prozent beurteilen.⁴³ Ähnlich verhält es sich bei der Frage was mit persönlichen Daten passiert, die man z.B. in sozialen Netzwerken angibt. 20 Prozent der Intensiv-Nutzer geben an, dies gut einschätzen zu können, bei den Internet-Nutzern insgesamt sind es nur mehr 15 Prozent.⁴⁴

Sehr eindrucksvoll zeigt die Studie auch, dass zwar 84 Prozent der Internet-Nutzer der Meinung sind, dass viele Nutzer zu sorglos persönliche Daten von sich preisgeben, dem entgegen sind aber 70 Prozent überzeugt sind, dass das bei ihnen selbst nicht der Fall ist (22% geben an dieses Gefühl zu haben). Die Ergebnisse ähneln sich hierbei in allen Altersklassen. Im Hinblick auf die Datenschutzrichtlinien zeigt die DIVISI Studie, dass rund die Hälfte der bundesdeutschen Bevölkerung, welche Internetkäufe tätigen, in der Regel, bzw. ab und zu die allgemeinen Geschäftsbedingungen, bzw. Datenschutzbestimmungen bei einem online Einkauf liest.⁴⁵

Auf einzelne Aktivitäten aufgrund von eigenen Sicherheitsmaßnahmen zu verzichten, sind Internetnutzer unter 30 Jahren hingegen nicht sehr bereit. Während 16 Prozent auf eine Mitgliedschaft in sozialen Netzwerken verzichten, sind es immerhin 32 Prozent, welche eine Speicherung von eigenen Dateien (Fotos, Dokumente) unterlassen. Das Nicht-Versenden von vertrauenswürdigen Informationen per E-Mail betreiben immerhin 37 Prozent der unter 30-Jährigen.⁴⁶

Alice E. Marwicks und Danah Boyds aktuelle Forschungsergebnisse im Bereich Jugend und Onlineverhalten in sozialen Netzwerken zeigen, welche Praktiken und Strategien Jugendliche anwenden, um sich in sozialen Netzwerken im Bereich der Privatsphäre zu schützen. Die Ergebnisse ihrer Studie *Networked privacy: How teenagers negotiate*

⁴¹ Vgl. DIVISI Studie, 2013. S. 29

⁴² Vgl. DIVISI Studie, 2013. S. 34

⁴³ Vgl. DIVISI Studie, 2013. S. 34

⁴⁴ Vgl. DIVISI Studie, 2013. S. 34

⁴⁵ Vgl. DIVISI Studie, 2013. S. 38

⁴⁶ Vgl. DIVISI Studie, 2013. S. 42

*context in social media*⁴⁷ verweisen darauf, dass Jugendliche nicht nur technische Möglichkeiten des Datenschutzes, sondern auch anderen Methoden wie zum Beispiel die Steganographie verwenden, um nur bestimmte Inhalte mit den jeweiligen Adressanten zu teilen.⁴⁸ Ausschlaggebend für den Schutz der eigenen Daten ist nicht, ob man etwas veröffentlicht oder nicht, sondern das tiefgehende Verständnis des Kontextes, in dem die eigenen Daten im Netzwerk stehen. Um Datenschutz in einem Netzwerk zu erreichen, bedarf es des Verständnisses des Kontextes, sowie der Einflussnahme, technischer und semantischer Dimension, wie Informationen interpretiert werden.⁴⁹ Marwick und Boyd kommen zum Schluss, dass es für Jugendliche schwer ist, eine effiziente Kontrolle des Informationsflusses zu erlangen. Sie verwiesen auch darauf, dass die technischen Möglichkeiten zur Kontrolle des Informationsflusses in Netzwerken unzureichend für einen umfassenden Datenschutz sind.⁵⁰

Das Thema Big Data und dessen Folgen behandelt kurz der Artikel von Pieter Kleve und Richard De Mulder. Sie suchen darin nach einem neuen Gleichgewicht zwischen dem Recht auf Information und dem Schutz der eigenen Privatsphäre.⁵¹ Die Autoren bemängeln den Stellenwert der Privatsphäre heute. Das Recht auf Privatsphäre wird nämlich nicht nur der kompletten persönlichen Freiheit geopfert, sondern steht auch zum Teil im Widerspruch zu dem Recht an Informationen. Zum Thema Big Data diskutieren die Autoren kontrovers, denn einerseits weisen sie darauf hin, dass die heutigen Informationstechnologien auch missbraucht werden können, andererseits scheint es ihnen nicht ratsam aus Sorge vor Missbrauch die Sammlung der persönlichen Daten zu unterlassen.⁵²

Da mit Hilfe von Big Data aus anonymisierten Daten Personen re-identifiziert werden können oder auch persönliche Daten gewonnen werden können, erklären Paul M. Schwartz und Daniel J. Solove in *The PII Problem: Privacy and a New Concept of*

⁴⁷ Vgl. Marwick, Alice E.; Boyd, Danah (2014): Networked privacy: How teenagers negotiate context in social media. In: *New Media & Society* 16 (7). S. 1051-1067. Abrufbar unter: <http://nms.sagepub.com/content/16/7/1051.full> (10.01.2015)

⁴⁸ Vgl. Marwick; Boyd, 2014. S. 1056, 1058

⁴⁹ Vgl. Marwick; Boyd, 2014. S. 1063

⁵⁰ Vgl. Marwick; Boyd, 2014. S. 1064

⁵¹ Vgl. Kleve, Pieter; De Mulder, Richard (2008): Privacy protection and the right to information: In search of a new balance. In: *Computer Law and Security Report*. 24 (3). S. 223-232 Abrufbar unter: <http://www.sciencedirect.com/science/article/pii/S0267364908000381> (03.07.2014)

⁵² Vgl. Kleve; De Mulder, 2008. S. 231

Personally Identifiable Information eine Möglichkeit, wie Daten auch im Zeitalter von Big Data – zwar mit einem Risiko der Re-Identifikation – anonymisiert werden können.⁵³ Sie rufen zu einem unterschiedlichen Umgang mit den unterschiedlichen Arten von Daten auf. Auf einer Skala zwischen den identifizierten Daten auf der einen Seite und den nicht identifizierbaren Daten auf der anderen, müssen identifizierbare sowie identifizierte Daten besser geschützt werden.⁵⁴

3. Grundlegende kommunikationswissenschaftliche Theorie

Wieso das Wissen der Konsumenten eine derart große Rolle spielt, wird hier mit der dem Konstruktivismus, der konstruktivistischen Medientheorie, sowie dem kommunikativen Konstruktivismus begründet.

3.1. Konstruktivismus

Bentele, Brosius und Jarren definieren den Konstruktivismus als Summe unterschiedlicher Denkrichtungen, die der Gedanke vereint, dass die objektive Realität grundsätzlich unzugänglich sei.⁵⁵ Das Kernproblem besteht dabei in der Beobachtung und Herausarbeitung der prozessual verstandenen Entstehung von Wirklichkeit.⁵⁶ Sich auf die naturalistische Kognitionstheorie berufend, gehen Konstruktivisten davon aus, dass man als Wahrnehmender nicht hinter seine eigene Wahrnehmung blicken könne.⁵⁷ „Während der Konstruktivismus generell davon ausgeht, dass die Wirklichkeit keine bloße ‚positive‘ Gegebenheit darstellt, sondern eine, wenn auch keineswegs beliebige Konstruktion ist, [...] variiert die Frage quer über die Disziplinen, wie und was konstruiert wird.“⁵⁸ Aus Sicht der Sozialwissenschaftler und Soziologen Berger und Luckmann ist die

⁵³ Vgl. Schwartz, Paul M.; Solove, Daniel J. (12/2011): The PII Problem: Privacy and a New Concept of Personally Identifiable Information. In: New York University Law Review, 86 (6). S. 1814-1894. Abrufbar unter: <http://www.nyulawreview.org/sites/default/files/pdf/NYULawReview-86-6-Schwartz-Solove.pdf> (23.01.2015)

⁵⁴ Vgl. Schwartz; Solove, 2011. S: 1877f.

⁵⁵ Vgl. Bentele, Günter; Brosius, Hans-Bernd; Jarren, Otfried (Hrsg.) (2013): Lexikon Kommunikations- und Medienwissenschaft. 2. Überarbeitete und erweiterte Auflage. Wiesbaden: Springer Fachmedien. S. 155

⁵⁶ Vgl. Pörksen, Bernhard (2014): Konstruktivismus. Medienethische Konsequenzen einer Theorie-Perspektive. Wiesbaden: Springer Fachmedien. S. 1

⁵⁷ Vgl. Bentele; Brosius; Jarren; 2013. S. 155 und Vgl. Pörksen, 2014. S. 1

⁵⁸ Keller, Reiner; Knoblauch, Hubert; Reichertz, Jo (Hrsg.) (2013): Kommunikativer Konstruktivismus. Theoretische und empirische Arbeiten zu einem neuen wissenschaftssoziologischen Ansatz. Wiesbaden: Springer Fachmedien. S. 9

Konstruktion ein sozialer Prozess und die Wirklichkeit demnach eine gesellschaftliche Konstruktion.⁵⁹

3.2. Konstruktivistische Medientheorie

Ausgangspunkt des konstruktivistischen Mediendiskurses ist die Frage „ob Massenmedien die Realität angemessen wiedergeben, bzw. ob und inwieweit sie überhaupt imstande sind, dies zu tun.“⁶⁰ Burkart schreibt dazu, dass die Realität nur sehr entfernt etwas mit dem zu tun hat, was die Medien berichten.⁶¹ Wir konstruieren durch Bewusstseinsleistungen Wirklichkeitsvorstellungen, wobei es außerhalb unserer kognitiven Wirklichkeit eine Realität gibt, die Anlass für unsere Wirklichkeitskonstruktionen bietet. Wie die Realität an sich ist, das entzieht sich unserer Erkenntnismöglichkeit, da wir nur jene Wirklichkeit kennen, die wir wahrnehmen.⁶² Unsere kognitive Wirklichkeit ist daher immer mit einer Interpretation unserer eigenen Wahrnehmung.

Wenn dies nun auf den Bereich der Kommunikation und die Medien adaptiert wird, so sind Medienangebote niemals Abbilder von Wirklichkeit. „Wirklichkeit ist in einer von Massenmedien geprägten Gesellschaft also zunehmend das, was wir über Mediengebrauch als Wirklich konstruieren, dann daran glauben und entsprechend handeln und kommunizieren“.⁶³

Wenn Medien nun zu wenig oder gar nicht über Datenspeicherung und -Analyse berichten, so sind die Fakten, aber auch die Möglichkeiten von Big Data für viele Rezipienten unwirklich und fernab des Vorstellungsvermögens.

⁵⁹ Vgl. Keller; Knoblauch; Reichertz (Hrsg.), 2013. S. 9f.

⁶⁰ Burkart, Roland (2002): Kommunikationswissenschaft. Grundlagen und Problemfelder. Umriss einer interdisziplinären Sozialwissenschaft. 4., überarbeitete und aktualisierte Auflage. Wien: Böhlau Verlag. S. 302

⁶¹ Vgl. Burkard, 2002. S. 303

⁶² Vgl. Schmidt, Siegfried (1990): Wir verstehen uns doch? Von der Unwahrscheinlichkeit gelingender Kommunikation. In: Deutsches Institut für Fernstudien an der Universität Tübingen (Hrsg.): Funkkolleg. Medien und Kommunikation. Konstruktionen von Wirklichkeit. Studienbrief 1. Weinheim, Basel: Beltz Verlag. S. 54.

⁶³ Schmidt, Siegfried (1994): Die Wirklichkeit des Beobachters. In: Merten; Klaus; Schmidt, Siegfried J.; Weischenberg, Siegfried (Hrsg.): Die Wirklichkeit der Medien. Eine Einführung in die Kommunikationswissenschaft. Opladen: Westdeutscher Verlag GmbH. S. 18.

3.3. Kommunikativer Konstruktivismus

Auch der kommunikative Konstruktivismus schließt an diese Theorie der gesellschaftlichen und medialen Konstruktion von Wirklichkeit an. Es ist ein theoretischer Ansatz, der auf dem Sozialkonstruktivismus aufbaut, der von Berger und Luckmann 1966 begründet wurde.⁶⁴ Durch die Betonung der Kommunikation geht es hier jedoch darum, die kommunikativen Prozesse (face-to-face wie auch medial) „der sozialen Konstruktion der Wirklichkeit in den Vordergrund zu rücken“.⁶⁵ Stand am Anfang noch die Sprache und der sprachliche Austausch als zentrale Trägerin des gesellschaftlichen Wissens im Vordergrund, so konzentrierte sich das empirische Forschungsvorhaben immer weiter auf die Kommunikation.⁶⁶ Kommunikatives Handeln konstruiert Bewusstsein. Wenn das Bewusstsein die Erfahrung mit dem einen und anderen vergleicht, dem es entweder ähnelt oder sich unterscheidet, haben wir es mit Sinn zu tun. Sinn wird erst durch das Bewusstsein gebildet.⁶⁷ Hubert Knoblauch postuliert dazu, dass das Wissen im Grunde ein sozial vermittelter Sinn ist.⁶⁸ „Der Sinn, aus dem das Wissen zehrt, erhält seine Bestätigung nicht aus einer ihm zugrundeliegenden Erfahrung, sondern erweist sich als relevant, weil er Handlungen leitet.“⁶⁹ Wissen ist damit nichts was vom Handeln getrennt werden kann. Laut seiner Definition wird Handeln wesentlich durch Sinn bestimmt. „Wissen ist der sozial vermittelte und verfügbare Sinn, der das Handeln aufgrund seiner Sozialität zum kommunikativen Handeln macht.“⁷⁰ Aus soziologischer Sicht wird somit sowohl das Wissen, als auch das Handeln gesellschaftlich begründet, jedoch warnt Knoblauch davor, Wissen in der Sozialität aufgehen zu lassen. Es ist nicht nur Kommunikation, aber etwas, das der Kommunikation unterstellt ist. Wissen als sozialen Sinn anzusehen ist jedoch nötig, weil es nicht nur Bewusstsein benötigt, sondern auch ein Subjekt.⁷¹ Sinn ist dabei jedoch kein Inhalt, sondern eine Bezugnahme auf etwas, vor dem Hintergrund von Anderem und Ähnlichem.⁷²

⁶⁴ Vgl. Keller; Knoblauch; Reichertz (Hrsg.), 2013. S. 26 sowie: Berger, Peter L.; Luckmann, Thomas (1966/1969): Die gesellschaftliche Konstruktion der Wirklichkeit. Eine Theorie der Wissenssoziologie. Frankfurt am Main: S. Fischer Verlag GmbH. S. 197

⁶⁵ Keller; Knoblauch; Reichertz (Hrsg.), 2013. S. 12

⁶⁶ Vgl. Keller; Knoblauch; Reichertz (Hrsg.), 2013. S. 25

⁶⁷ Vgl. Knoblauch, Hubert (2014): Wissenssoziologie. 3. Auflage. Konstanz und München: UVK-Verlagsgesellschaft. S. 352

⁶⁸ Vgl. Knoblauch, 2014. S. 352 f.

⁶⁹ Knoblauch, 2014. S. 351

⁷⁰ Keller; Knoblauch; Reichertz (Hrsg.), 2013. S. 36

⁷¹ Vgl. Knoblauch, 2014. S. 353

⁷² Vgl. Knoblauch, 2014. S. 352

4. Das Konstrukt Wissen

Da diese Arbeit das Wissen der Smartphone-Nutzer untersuchen möchte, bedarf es zu aller erst einer Beschreibung des Wissensbegriffs. Obwohl Wissen umgangssprachlich sehr oft gebraucht wird, besteht zwischen den Wissenschaftsdisziplinen wie Philosophie, Psychologie, Sozialwissenschaft, Linguistik usw. keine einheitliche und allgemein gültige Definition von Wissen.⁷³ Daher werden hier wichtige Merkmale und Klassifikationen von Wissen erörtert, die den Zustand des Wissens bestmöglich beschreiben.

4.1. Die Vermittlung von Wissen in der Gesellschaft

Im Bereich der Wissenssoziologie wird Wissen, laut Hubert Knoblauch, wie vorher erwähnt, als sozial vermittelter Sinn verstanden.⁷⁴ Wissen wird, laut Alfred Schütz, nicht von jedem einzelnen neu konstruiert, sondern vieles wird durch den Sinn sozial abgeleitet. „Sozial abgeleitetes Wissen bedeutet, dass fast alles, was wir erfahren, von anderen übernommen wird.“⁷⁵ Wie bestimmte Objekte aussehen, wie man Geräte benutzt, wie man sich verhält, wird sozial vermittelt. Somit ist Wissen, vereinfacht gesagt, „der sozial gewordene Sinn“.⁷⁶ Wissen wird nicht nur in der Schule vermittelt, sondern auch im täglichen Leben angereichert, nämlich dann, wenn wir von anderen etwas übernehmen. Selbst Emotionen beruhen auf und bestehen aus Wissen. Welche Voraussetzungen es braucht, um neues Wissen zu adaptieren wird im folgenden Teil genau erklärt.

4.2. Die Entwicklung von Daten, über Informationen, hin zu Wissen

Nicht nur, weil Daten, Informationen und Wissen zentrale Begriffe dieser Arbeit sind, benötigt es eine klare Abgrenzung, sondern auch deshalb, weil diese Begriffe im Alltag häufig alle als Wissen bezeichnet werden. Notwendig wurde diese Abgrenzung durch die Informationstechnologie, welche die Begriffe sehr technisch definiert.⁷⁷ Daten sind

⁷³ Siehe dazu: Hasler Roumois, Ursula (2007): Studienbuch Wissensmanagement. Grundlagen der Wissensarbeit in Wirtschafts-, Non-Profit- und Public-Organisationen. Zürich: Orell Füssli Verlag Ag. S. 29. Sowie: Aulinger, Andreas; Fischer, Dirk (2000): Einige Daten und Informationen zum Wissensmanagement. DBW. Die Betriebswirtschaft, 60 (5). Seite 645. Abrufbar unter: http://www.wiso-net.de/webcgi?START=A20&T_FORMAT=5&DOKM=1000436_ZECU_0&TREFFER_NR=1&WID=16152-3420944-51924_1 (22.05.2014)

⁷⁴ Vgl. Knoblauch, 2014. S. 352 f.

⁷⁵ Knoblauch, 2014. S. 353

⁷⁶ Knoblauch, 2014. S. 353

⁷⁷ Vgl. Hasler Roumois, 2007. S. 33

demnach Zeichen, die aus einem Zeichenvorrat nach bestimmten Regeln (Syntax) zu festen Zeichenverbänden kombiniert werden. Während Daten materiell wahrnehmbar sind, haben Informationen eine immateriell und dynamische Qualität.⁷⁸ Daten, erklärt Ursula Halser Roumois, werden dann für den Menschen zu Informationen, wenn er ihre Bedeutung in einem Kontext versteht und somit ihre Relevanz für sein aktuelles (Wissens-)Bedürfnis erkennt.⁷⁹ „Das bedeutet, dass Information nicht losgelöst von einem Kontext und einem lernenden oder erkennenden Subjekt beschrieben werden kann. Ob Daten, die eine Person wahrnimmt, zu Informationen werden, hängt also davon ab, ob die Person sie in einer konkreten Kommunikationssituation braucht.“⁸⁰

Im Alltag bezeichnen wir Daten oft schon als Informationen. So kann man genaugenommen über sich keine Informationen, sondern wenn, dann nur Daten preisgeben, die in einem weiteren Schritt erst zu Informationen konstruiert werden müssen. Aber auch im Hinblick auf das Wissen der Konsumenten über die Sammlung ihrer Daten, werden Daten aus den rezipierten Medien erst dann zu Informationen, wenn man das bestehende Wissen mit dem aktuellen Bedürfnis vergleicht und die Informationsqualität der Daten für sich erkennt.⁸¹ Sobald Daten für den Menschen eine Informationsqualität haben, wird die wahrgenommene Information mit dem vorhandenen Wissen vernetzt. „Durch den Prozess des Aufnehmens und Verknüpfens schafft der Mensch in seinem Kopf neues Wissen.“⁸² Wissen wird als dritter Baustein in der Daten-Information-Wissens-Triade von Hasler Roumois als immateriell, nicht greifbar, subjektiv und nur im Kopf eines Menschen existierend bezeichnet.⁸³

4.3. Die Dimensionen des Wissens

Da bei dieser Untersuchung das Wissen der UntersuchungsteilnehmerInnen bestimmt werden möchte, ist eine Unterscheidung in die Dimensionen implizites und explizites Wissen notwendig. Wissen kann nur im Kopf einer Person vorkommen und ist somit streng genommen immer implizit.⁸⁴ Wissen, bzw. potentielle Information kann in Form von Daten artikuliert und somit Teile des Wissens externalisiert werden. Explizites

⁷⁸ Vgl. Hasler Roumois, 2007. S. 33f.

⁷⁹ Vgl. Halser Roumois, 2007. S. 34

⁸⁰ Halser Roumois, 2007. S. 34

⁸¹ Vgl. Hasler Roumois, 2007. S. 34

⁸² Hasler Roumois, 2007. S. 35

⁸³ Vgl. Hasler Roumois, 2007. S. 36

⁸⁴ Vgl. Hasler Roumois, 2007. S. 39f.

Wissen bedeutet daher expliziertes implizites Wissen.⁸⁵ Laut dem Wissenschaftstheoretiker Michael Polanyi wissen wir allerdings viel mehr als wir aussprechen können, denn implizites Wissen umfasst alles, „was eine Person aufgrund ihrer Erfahrung, ihrer Geschichte, ihrer Tätigkeit und ihres Lernens im Kopf hat.“⁸⁶ Implizites Wissen wird an dieser Stelle in drei Bewusstheitszustände eingeteilt, wobei diese Unterteilung willkürlich ist, denn im Grunde handelt es sich um einen kontinuierlichen Verlauf des Wissens von völlig unbewusst zu bewusst. Dennoch ist eine Unterteilung hilfreich, als dass für einen bestimmten Wissensinhalt ein bestimmter Bewusstseinszustand typisch und entscheidend ist, ob dieses Wissen überhaupt expliziert werden kann.⁸⁷

- Bewusstes Wissen („Ich weiß, dass ich es weiß“, bzw. „Ich weiß, dass ich es nicht mehr weiß“) wurde bewusst gelernt, ist kognitiv verfügbar und kann somit expliziert werden, es sei denn man hat es vergessen, wessen man sich aber bewusst ist. *Know-that, Know-about, Know-why und eventuell Know-what-to-do gehören zum bewussten Wissen.*⁸⁸
- Latentes Wissen („Ich ahne, dass ich es weiß“) wurde nicht bewusst gelernt, jedoch ist es potentiell aktivierbar und somit externalisierbar.
- Stilles Wissen („Ich weiß nicht, dass ich es weiß“) umfasst den gesamten Rest unseres Wissens, das so tief verwurzelt ist, dass wir es als gegeben annehmen und nicht erklärbar ist, sondern höchstens gezeigt werden kann.⁸⁹

4.4. Die Wissensarten

Neben den impliziten und expliziten Wissen kann man auch unter dem prozeduralen Wissen (Know-how) und dem deklarativen Wissen (Know-that) unterscheiden. Während das erstere Handlungs-, Erfahrungs-, Anwendungswissen sowie Können, Fertigkeit und Fähigkeit beinhaltet und daher schwer zu explizieren ist, kann das deklarative Wissen (Fakten-, Sach-, Allgemeinwissen) sehr gut expliziert werden.⁹⁰ In dieser Arbeit wird somit das deklarative Wissen zum Untersuchungsgegenstand, wobei hier unter dem Faktenwissen und dem Kontext- und Strukturwissen unterschieden wird. Obwohl, wie

⁸⁵ Vgl. Hasler Roumois, 2007. S. 43

⁸⁶ Halser Roumois, 2007. S. 39

⁸⁷ Vgl. Hasler Roumois, 2007. S: 42

⁸⁸ Vgl. Hasler Roumois, 2007. S: 40f.

⁸⁹ Vgl. Haler Roumois, 2007. S. 41

⁹⁰ Vgl. Hasler Roumois, 2007. S. 45f.

Werner Wirth schreibt, es schwer ist Informationen bzw. Daten dem Fakten- bzw. Strukturwissen zuzuteilen, weil die Strukturiertheit einer Information von der Darstellung und nicht von der Wirklichkeit abhängt⁹¹, so ist es besonders beim Thema Big Data sehr zentral, ob allein die Datenspeicherung und –Analyse, oder auch das dahinterstehende Ziel der Vorhersagbarkeit des Verhaltens sowie deren Folgen erkannt werden. Da Faktenwissen über Big Data allein noch nicht ausreicht, um den Umfang und die Folgen in der Zukunft zu erkennen, wird ebenso das Strukturwissen abgefragt. Für diese Untersuchung umfasst das Faktenwissen somit die Kenntnis über die Speicherung und Analyse von Daten, während das Strukturwissen das Wissen der Zusammenhänge impliziert.

5. Big Data

5.1. Begriffsdefinition

Big Data bedeutet wortwörtlich riesige Datenmengen, eine exakte Definition, wie groß der Umfang ist, ab dem man von Big Data spricht, gibt es nicht.⁹² Edd Dumbill definiert in *Planning for Big Data* den neuen Modebegriff: „Big Data sind Daten, deren Verarbeitung die Kapazität konventioneller Datenbanksysteme übersteigt.“⁹³ Der Begriff bezeichnet neben den Daten selbst auch die neuen Technologien und Datenarchitekturen, die es ermöglichen, Werte für Vorhersagen aus großen Datenmengen unterschiedlicher Struktur mit Hilfe von Hochgeschwindigkeitsverarbeitung und Analyse zu generieren.⁹⁴ Vincent McBurney nennt unterschiedliche Quellen, die den Begriff in seiner aktuellen Verwendung geprägt haben können.⁹⁵ Woher der Begriff allerdings stammt und wann er erstmals im aktuellen Kontext verwendet wurde, ist nicht eindeutig identifizierbar.

⁹¹ Vgl. Wirth, Werner (1997): Von der Information zum Wissen. Die Rolle der Rezeption für die Entstehung von Wissensunterschieden. Ein Beitrag zur Wissensklutforschung. Opladen: Westdeutscher Verlag. S. 103

⁹² Vgl. Klausnitzer, 2013. S. 9 und S. 89

⁹³ Dumbill, Edd (2012): *Planning for Big Data. A CIO's Handbook to the Changing Data Landscape*. Sebastopol: O'Reilly Media. S. 9. Abrufbar unter: http://cdn.oreillystatic.com/oreilly/radarreport/0636920025559/Planning_for_Big_Data.pdf (23.01.2015)

⁹⁴ Vgl. Klausnitzer, 2013. S. 89

⁹⁵ Vgl. McBurney, Vincent (31.05.2012): The Origin and Growth of Big Data Buzz. Toolbox for IT Blog. Abrufbar unter: <http://it.toolbox.com/blogs/infosphere/the-origin-and-growth-of-big-data-buzz-51509> (09.05.2014)

5.2. Was ist Big Data?

Derzeit erleben wir eine noch nie dagewesene Datenrevolution, sind aktiv mit dabei und dennoch „sind die tiefgehenden Veränderungen, die damit einhergehen, den meisten von uns nicht bewusst.“⁹⁶ Denn es fehlt nicht nur die breite gesellschaftliche Aufmerksamkeit, die eigentlich notwendig wäre, sondern, so erklären Constanze Kurz und Frank Rieger, ohne wenigstens einem intuitiven Verständnis für technische Systeme, ihre Grundlagen und Funktionsweisen ist es schwer, die Risiken der zunehmenden Digitalisierung überhaupt erst zu verstehen, geschweige denn die eigene (digitale) Zukunft selbst in die Hand zu nehmen.⁹⁷ Als ausschlaggebend für ein Verständnis der digitalen Welt geben sie das Durchblicken der finanziellen Mechanismen an, womit die resultierenden Motivationen der Menschen und Institutionen erkannt werden können.⁹⁸ Sie erklären mit dem „Bezahlen mit Daten“ – Modell „wie teuer ‚kostenlos‘ wirklich ist“.⁹⁹

Die Einschätzung darüber, wie viele Daten über jeden einzelnen von uns gesammelt, gespeichert und analysiert werden, liegt außerhalb unserer Vorstellungskraft. Viktor Mayer-Schönberger und Kenneth Cukier verweisen darauf, dass Big Data jenen, die Daten analysieren, wertvolle Einsichten geben kann. Deshalb sind sie überzeugt, dass das Speichern und Analysieren unserer persönlichen Daten weiterhin zunehmen wird.¹⁰⁰ „Größe und Umfang der gesammelten Daten werden sprunghaft wachsen, weil die Kosten für die Speicherung weiter dramatisch sinken und die Analysewerkzeuge immer mächtiger werden.“¹⁰¹ Im Hintergrund der digitalen Revolution wird unsere Welt mathematisiert und mit Algorithmen berechnet. Aus den riesigen Datenmengen kann somit ein recht konkretes Bild von dem geschaffen werden, was wir in Vergangenheit getan haben, in der Gegenwart tun und vor allem, was wir in Zukunft tun werden.¹⁰² Mit technischer Hilfe und unseren oft freiwillig bereitgestellten Daten wird das menschliche Verhalten vorhersagbar und somit wir berechenbar. Der ungarische Physikprofessor und Experte für Netzwerk-Wissenschaften, Albert-László Barabási ist überzeugt, dass einige unserer Verhaltensweisen, von denen wir bis jetzt der Meinung waren, dass sie zufällig

⁹⁶ Klausnitzer, 2013. S. 7

⁹⁷ Vgl. Kurz, Constanze; Rieger, Frank (2011): Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. Frankfurt am Main: Fischer Verlag. S. 9

⁹⁸ Vgl. Kurz; Rieger, 2011. S. 9

⁹⁹ Kurz; Rieger, 2011. S. 14ff.

¹⁰⁰ Vgl. Mayer-Schönberger; Cukier, 2013. S. 190

¹⁰¹ Mayer-Schönberger; Cukier, 2013. S. 190

¹⁰² Vgl. Klausnitzer, 2013. S. 7

seien, vorhersagbaren Gesetzen folgen.¹⁰³ Ein Beispiel wie genau unser Verhalten vorhersagbar ist, liefern uns seine Ergebnisse von Experimenten zu Mobilitätsprognosen. Das Maximum an Vorhersagbarkeit lag dabei bei 93 Prozent, doch viel erstaunlicher ist, dass die Vorhersagbarkeit in der gesamten Untersuchungsreihe bei niemandem unter 80 Prozent lag.¹⁰⁴ Ähnliche Ergebnisse erhielt Adam Sadilek von der Rochester Universität in New York. Er entwickelte ein System, mit dem er den Standort eines Twitter-Nutzers vorhersagen konnte. Die individuellen Bewegungsdaten von ein paar Wochen kombiniert mit den Bewegungsprofilen von den zwei engsten Twitter-Freunden reichen aus, um den Standort einer Person auf einem 100-Meter Radius mit 77 prozentiger Genauigkeit zu bestimmen. Die Vorhersagegenauigkeit stieg auf 85 Prozent, wenn die Angaben von neun Twitter-Freunden kombiniert wurden. Und selbst wenn ein Twitter-Nutzer noch nie seinen Standort geteilt hat, kann sein Standort mit 47 Prozent Genauigkeit festgelegt werden, wenn Informationen von zwei Freunden zur Verfügung stehen, und mit 57 Prozent, wenn die Informationen von neun Freunden vorhanden sind. Dies gilt nicht nur für Twitter, auch Facebook-Freunde können sehr viel über die eigene Identität preisgeben, warnt Sadilek.¹⁰⁵

Der immer präziser werdende Blick in die Zukunft nennt sich vorausschauende Datenanalyse, „Predict Analytics“.¹⁰⁶ Und genau in dieser Möglichkeit „aus den Informationen der Vergangenheit Ihr ganz persönliches Verhalten in der Zukunft vorherzusagen“¹⁰⁷ sieht Roman Maria Koidl das Problem. Denn erstens haben wir keine Kontrolle mehr über die Verwendung unserer Spuren vergangener Aktivitäten, und zweitens liegen diese Daten in den Händen eines Systems über das niemand demokratisch seine Zustimmung erteilt hat.¹⁰⁸ Die Folge wird sein, dass dieses System in Zukunft darüber entscheidet, „ob wir eine Versicherung bekommen, kreditwürdig sind, eine Wohnung mieten dürfen, oder die Genehmigung erhalten, in bestimmte Länder

¹⁰³ Vgl. Song, Chaoming; Qu, Zehui; Blumm, Niclas; Barabási, Albert-László (19.02.2010): Limits of Predictability in Human Mobility. *Science*, 327. S. 1018-1021

Abgerufen unter: http://www.barabasilab.com/pubs/CCNR-ALB_Publications/201002-19_Science-Predictability/201002-19_Science-Predictability.pdf (20.05.2014)

¹⁰⁴ Vgl. Song et al., 2010. S. 1021

¹⁰⁵ Vgl. Aron, Jacob (25.01.2012): New Scientist. What your online friends reveal about where you are. Abgerufen unter: http://www.newscientist.com/article/mg21328495.500-what-your-online-friends-reveal-about-where-you-are.html#.VBcVUFck_u2 (15.09.2014)

¹⁰⁶ Vgl. Klausnitzer, 2013. S. 9

¹⁰⁷ Koidl, Roman Maria (2013): WebAttack. Der Staat als Stalker. Ein Besinnungsaufsatz. Essay. 2. Auflage. München: Wilhelm Goldmann Verlag. S. 11

¹⁰⁸ Vgl. Koidl, 2013. S. 11 f.

einzureisen.“¹⁰⁹ Welche Risiken Big Data mit sich bringt wird im Kapitel „Möglichkeiten, Risiken und Folgen von Big Data“ behandelt.

5.3. Woher kommen die Daten?

Die Datensammlung, die mittlerweile ein tsunamiartiges Ausmaß erreicht hat, wie es der österreichische Kommunikationsexperte, Rudi Klausnitzer beschreibt, beginnt schon vor unserer Geburt, z.B. in Form von Ultraschallbildern. Egal, was und wo wir etwas machen, es gibt praktisch keine Tätigkeit mehr, bei der wir keine Datenspuren hinterlassen, erklären Constanze Kurz und Frank Rieger.¹¹⁰ „Die Digitalgesellschaft macht vor kaum einem Lebensbereich halt – und sie erzeugt immer mehr Daten, die ausgewertet, analysiert, gefiltert und verarbeitet werden können.“¹¹¹ Täglich produzieren wir 2,5 Quintillionen Bytes.¹¹² Dabei geben wir Daten über uns preis, freiwillig, wie auch unfreiwillig, von denen wir nicht einmal ahnen, dass diese in der Zukunft verwendet werden (könnten).¹¹³ Das Big Data-Netzwerk wird aus verschiedenen Datenquellen gespeist. Klausnitzer nennt hier fünf Quellen die zur Datenlawine führen. Zu ihnen gehören die Daten externer Sensoren, wie beispielsweise Daten von Überwachungskameras, Mautstellen, Skilift- und Navigationssystemen.¹¹⁴ Die Business-Daten, welche Daten von Unternehmen und Behörden einbeziehen. Darunter fallen Kundenkartenprogramme, Kaufvorgänge mit elektronischen Zahlungsmitteln, jeder Online-Kontakt, Telefongesellschaftsdaten, und unzählige mehr.¹¹⁵ Als dritte Quelle nennt Klausnitzer die Social-Media-Daten, die meistens freiwillig öffentlich zur Verfügung gestellt werden und die wegen ihrer mangelnden Strukturiertheit bisher besonders schwierig einzuordnen und zu analysieren waren.¹¹⁶ Bei den Mobile-Daten sind jene Daten gemeint, „die von Hundertausenden von unterschiedlichen Applikationen und Sensoren in diesen Mobiltelefonen geliefert werden.“¹¹⁷ Abschließend nennt Klausnitzer die Suchmaschinen-Daten und externe Internetdaten, die wichtige Quellen für die Big Data-Analysen bilden. „Google Flu Trends, das erfolgreiche globale

¹⁰⁹ Koidl, 2013. S. 12

¹¹⁰ Vgl. Kurz; Rieger, 2011. S. 7

¹¹¹ Ebd. Kurz; Rieger, 2011. S. 7

¹¹² Vgl. Klausnitzer, 2013. S. 9

¹¹³ Vgl. Kurz; Rieger, 2011. S. 10

¹¹⁴ Vgl. Klausnitzer, 2013. S. 105

¹¹⁵ Vgl. Klausnitzer, 2013. S. 106

¹¹⁶ Vgl. Klausnitzer, 2013. S. 106

¹¹⁷ Klausnitzer, 2013. S. 106

Prognosemodell für Grippevorhersagen, (...) [habe] bereits das Potential bewiesen, das in diesen Daten liegt.“¹¹⁸ Kausalzusammenhänge sind dabei jene Zusammenhänge, die Aufschluss über verschiedenste Situationen geben können. Bei Google Flu Trends verweist Viktor Mayer-Schönberger und Kenneth Cukier jedoch auf die Tatsache, dass Big Data nur Korrelationen beschreibt, in diesem Fall Korrelationen bestimmter Suchbegriffe mit einer Grippewelle in einem bestimmten Gebiet. Diese Korrelation kann aber alle möglichen Ursachen haben, deshalb dürfen wir uns nicht von den Ergebnissen blenden lassen, denn Big Data sagt nichts über Kausalzusammenhänge aus.¹¹⁹

5.4. Möglichkeiten, Risiken und Folgen von Big Data

Ein grundlegendes Problem bei elektronisch gespeicherten Daten ist der Datenschutz und die Datensicherheit. Man könnte es so formulieren, dass Daten, die man ein Mal ins Internet stellt, für immer dort verloren sind, denn es kostet nicht nur Unmengen an Zeit und jede Menge Aufwand diese Daten wieder zu löschen, sondern es ist aufgrund ihrer möglichen weiteren Abspeicherung oder Weitergabe an Dritte beinahe eine Sache der Unmöglichkeit geworden, Daten zurückzuholen.

Nach dem NSA-Skandal, WikiLeaks und mittlerweile im Wochentakt wiederkehrende Enthüllungen über unrechtmäßige Verwendung von Daten, Datendiebstahl und vieles mehr, können wir uns unserer Daten nicht mehr sicher sein. „Es gibt keine sicheren Daten“¹²⁰, postuliert Roman Maria Koidl. Er verweist darauf, dass wir in Zukunft damit rechnen müssen, dass unsere Daten, die wir täglich bewusst oder unbewusst preisgeben, verwendet werden. Sei dies für gezielte Verkaufsaktionen, für kriminelle Handlungen oder für Vorhersagemodelle.¹²¹

Steffan Heuer und Pernille Tranberg beschreiben die persönlichen Daten als schwarzes Gold des 21. Jahrhunderts und erklären, dass sich viele Unternehmen im digitalen Goldrausch befinden und detaillierte Identitätsdatenbanken anlegen, um im Idealfall

¹¹⁸ Klausnitzer, 2013. S. 106

¹¹⁹ Vgl. Mayer-Schönberger; Cukier, 2013. S. 205 und S. 213

¹²⁰ Koidl, 2013. S. 38

¹²¹ Vgl. Koidl, 2013. S. 38

automatisch und in Sekundenbruchteilen ein komplettes Bild über jeden von uns zu erhalten.¹²² Sie schreiben dazu:

„Wundern sie sich nicht, wenn die Kassiererin im Supermarkt oder die Rezeptionsdame im Hotel weiß, wo Sie letzte Woche waren. Schließlich zieht die neue Kasse die Daten von ortsbezogenen Diensten und sozialen Netzwerken heran, in denen Sie aktiv sind, und kann sie mit einem biometrischen Gesichtsprofil sowie den neuesten Kreditkarteneinkäufen abgleichen. Sie werden wie üblich ihre Rechnung bezahlen. Aber je nach persönlichem Suchergebnis werden Sie vielleicht bevorzugt behandelt oder umgekehrt diesmal keinen Rabatt erhalten – alles abhängig von Ihrem jüngsten Online-Verhalten (...).“¹²³

Aber auch Viktor Mayer-Schönberger und Kenneth Cukier erklären, dass für manche Unternehmen die Daten in Wirklichkeit das Entscheidende sind für ihren Erfolg.¹²⁴ Mit Hilfe der Big Data Wertschöpfungskette zeigen sie eindrucksvoll auf, welche Korrelationen sich aus Datenanalysen ergeben können und wie diese dem jeweiligen Unternehmen wichtige Informationen zu geldsparenden Verbesserungen verhelfen können.¹²⁵ Denn „setzt man Big Data schlau ein, können sich das Geschäftsmodell eines Unternehmens und die Zusammenarbeit langjähriger Geschäftspartner völlig ändern“¹²⁶ womit auch Strukturveränderungen ganzer Wirtschaftszweige einhergehen können.¹²⁷

Vom Unternehmen zum Einzelnen, ist die versteckte und größte Bedrohung von Big Data für die breite Masse, die Möglichkeit der Vorhersagbarkeit unseres Verhaltens, unseres Aufenthaltsortes, unseres Gesundheitszustandes, kurz gesagt unseres Lebens. Aus Big Data-Analysen, die die Vorhersagen erst ermöglichen, ergeben sich auch Bürgerrechts- und Datenschutz-Aspekte. Im Hinblick auf „Predictive Policing“, bei dem Kriminalitätsprognosen mit Hilfe unserer Daten berechnet werden¹²⁸, schreibt Patrick Beuth in *Zeit Online*:

¹²² Vgl. Heuer, Steffan; Tranberg, Pernille (2013): Mich kriegt ihr nicht! Gebrauchsanweisung zur digitalen Selbstverteidigung. Hamburg: Murmann Verlag. S. 12

Vgl. dazu auch: Klausnitzer, 2013. S. 10

¹²³ Heuer; Tranberg, 2013. S. 12

¹²⁴ Vgl. Mayer-Schönberger; Cukier, 2013. S. 158

¹²⁵ Vgl. Mayer-Schönberger; Cukier, 2013. S. 158ff.

¹²⁶ Mayer-Schönberger; Cukier, 2013. S. 167

¹²⁷ Vgl. Mayer-Schönberger; Cukier, 2013. S. 182.

¹²⁸ Vgl. Klausnitzer, 2013. S. 34

Wenn (...) unschuldige Menschen das Gefühl haben, dass sie sich in einer Umwelt bewegen, in der ihr Verhalten vorausberechnet wird, dann hat dieses Wissen höchstwahrscheinlich Auswirkungen auf ihr Verhalten. Sie werden sich also anders benehmen, als wenn sie unbeobachtet wären – wären also nicht mehr frei in ihrer Entscheidung. In Deutschland zumindest wäre das verfassungsrechtlich bedenklich.¹²⁹

Aber auch Systeme, die unseren Gesundheitszustand in Echtzeit erfassen, können gefährlich werden. Wenn sie nämlich die erhaltenen Daten an Krankenkassen weitergeben, mit dem Ziel, dass Menschen, die aufgrund ihres Gesundheitszustandes weniger Kosten für das Versicherungsunternehmen erzeugen, eine günstigere Versicherung erhalten, oder im Gegensatz andere, die aufgrund eines schlechteren Zustandes ihrer Gesundheit sehr viele Kosten verursachen, bangen müssen, ob sie überhaupt erst eine Versicherung bekommen.¹³⁰

Dabei wirkt doch alles so harmlos, denn Daten gehen uns oft spielerisch von der Hand. Gamifizierung heißt hier das Zauberwort. Gamifizierte Informationen, sind Informationen, die mit Hilfe von Spielmechanismen erhoben werden. Durch die Spielmechanismen wird zum einen die Dopamin-Ausschüttung angeregt, zum anderen dient Gamifizierung der Verhaltenslenkung, denn es trägt zum Ausschluss von zufälligem Verhalten bei. Sobald der Algorithmus nämlich errechnet hat, wie wir uns verhalten, um das beste Ergebnis zu erbringen, dann steuert er sogleich die Spielelemente so, dass wir uns gerne und „freiwillig“ bemühen, das vorgegebene Ziel zu erreichen.¹³¹

Mayer-Schöneberger und Cukier sind überzeugt, dass Big Data bei verantwortungsvoller Nutzung zu einem nützlichen Werkzeug für rationale Entscheidungen werden kann, allerdings kann Big Data in den falschen Händen auch eine Diktatur der Daten bedeuten. Risiken, die Big Data mit sich bringt, sind laut ihnen zum einen die Gefahr, dass Menschen schon aufgrund ihres vorhergesagten Verhaltens bestraft werden, obwohl sie noch gar nicht gehandelt haben.¹³² Damit würden die menschliche Handlungsfreiheit,

¹²⁹ Vgl. Beuth, Partick (19.08.2011.): Die Polizei als Hellseher. In Kalifornien berechnet die Polizei voraus, wo Verbrechen geschehen werden und wartet dort auf Kriminelle. In Deutschland wäre das verfassungsrechtlich bedenklich. Zeit Online. 11:04 Uhr. Abrufbar unter: <http://www.zeit.de/digital/datenschutz/2011-08/predictive-policing> (21.05.2014)

¹³⁰ Vgl. R  th, Magdalena (14.03.2013): Dacadoo – „Gesundheit in Echtzeit“. Interview – Dacadoo will Gesundheit messbar machen und sich in diesem Sinne auch mit Krankenkassen zusammentun. Die Z  rcher im Frischlings-Interview. In: Gr  nderszene. Abrufbar unter: <http://www.gruenderszene.de/interviews/dacadoo> (21.05.2014) Siehe dazu auch: Koidl, 2013. S. 39 f.

¹³¹ Vgl. Klausnitzer, 2013. S. 25, 56

¹³² Vgl. Mayer-Sch  nberger, Cukier, 2013. S. 190

sowie die moralischen Grundsätze und die Verantwortung für das eigene Verhalten schwer geschädigt werden warnen die Autoren.¹³³ Sie verweisen aber auch darauf, dass der Schutz der Privatsphäre schwieriger wird, da sowohl Anonymisierungen wie auch das opt out (Nicht –Teilnehmen), bei genügend vorhandenen Daten, sich als nutzlos erweisen kann,¹³⁴ und auf den ersten Blick mit nicht personenbezogenen Daten, Rückschlüsse auf vertrauliche Details im Leben einer Person gezogen werden können.¹³⁵ Big Data entschlüsselt unsere persönlichsten Informationen, unseren Tagesablauf, unsere Gesundheit oder auch unser illegales Verhalten.¹³⁶ „Die zentrale Frage ist dabei nicht, ob Big Data die Gefährdung der Privatsphäre erhöht (das ist der Fall), sondern ob sich durch Big Data die Qualität dieser Gefahr verändert.“¹³⁷ Da es heute tatsächlich eine neue Qualität von Bedrohung gibt, nämlich dadurch, dass der Wert der Daten nicht nur in der durch sie generierten Information, sondern vorwiegend in der vielfachen Wiederverwendung der Daten liegt, erklären Mayer-Schönberger und Cukier welche Veränderungen der Datenschutzbestimmungen sie für sinnvoll erachten.¹³⁸ Dies wird im nächsten Kapitel erörtert.

Nichts desto trotz bringt Big Data neben den vielen Risiken auch Vorteile mit sich. Mayer-Schönberger und Cukier sehen Big Data als integralen Faktor, der für das Verständnis und die Lösung vieler drängender weltweiter Probleme herangezogen werden wird.¹³⁹ „Wenn man nämlich voraussagen kann, wie das eigene Handeln sich in der Zukunft wahrscheinlich auswirken wird, dann kann man rechtzeitig eingreifen, um Probleme zu vermeiden und Ergebnisse zu verbessern.“¹⁴⁰ Mayer-Schönberger und Cukier sehen Big Data-Vorhersagen nicht in Stein gemeißelt, sondern als Wahrscheinlichkeiten, was bedeutet, dass die Vorhersagen veränderbar sind – gerade auch durch uns.¹⁴¹ Die Anwendungsbereiche von Big Data werden sich auf immer mehr Lebensbereiche ausbreiten und auch helfen Alltägliches besser erledigen zu können. Es ist jedoch kein Zaubermittel, das Weltfrieden und allgemeinen Wohlstand hervorbringt.¹⁴²

¹³³ Vgl. Mayer-Schönberger, Cukier, 2013. S. 243

¹³⁴ Vgl. Mayer-Schönberger; Cukier, 2013. S. 194

¹³⁵ Vgl. Mayer-Schönberger; Cukier, 2013. S. 192

¹³⁶ Vgl. Mayer-Schönberger; Cukier, 2013. S. 192

¹³⁷ Mayer-Schönberger; Cukier, 2013. S. 192

¹³⁸ Vgl. Mayer-Schönberger; Cukier, 2013. S. 193

¹³⁹ Vgl. Mayer-Schönberger; Cukier, 2013. S. 243

¹⁴⁰ Mayer-Schönberger; Cukier, 2013. S. 245

¹⁴¹ Vgl. Mayer-Schönberger; Cukier, 2013. S. 246

¹⁴² Vgl. Mayer-Schönberger; Cukier, 2013. S. 244

Da die Autoren den größten Wert der Daten in ihrer Wiederverwendung und nicht im ursprünglichen Zweck sehen, für den sie womöglich gesammelt worden sind, sehen sie es als sinnvoll an, so viel Daten wie möglich zu sammeln und diese so lange zu speichern, wie sie wertvoll sind und bei Bedarf andere die Daten analysieren zu lassen.¹⁴³ Jedoch mahnen die Autoren Big Data als Werkzeug mit Demut und Menschlichkeit einzusetzen, da es niemals über vollkommene Information verfügen kann, und somit immer fehlbar bleiben wird.¹⁴⁴

6. Daten

6.1. Der Datenschutz – eine Reaktion auf technische Neuerungen

Wolfgang Schmale und Marie-Theres Tinnefeld schreiben zum Thema Datenschutz, dass dieser im 20. Jahrhundert als Reaktion auf die Entwicklung und Verbreitung der Computertechnologie entstand. Für die neuen technischen Entwicklungen waren neue Richtlinien erforderlich, denn sie wirken durch die weltweite Verdichtung der informationellen Kommunikationsmittel auf die Lebensbedingungen der Menschen ein.¹⁴⁵ Einander gegenüber stehen dabei die Interessen des Einzelnen am Schutz seiner Privatsphäre und den Bedarf der Gesellschaft an Informationen. Diese Interessen sind im Einzelfall gegeneinander abzuwägen.¹⁴⁶

6.1.1. Begriffsdefinition

Eine einheitliche Definition des Begriffs Datenschutzes fällt schwer. Zwar gibt die EU mit der Datenschutz-Richtlinie (RL 95/46/EG) die Bestimmungen für den Datenschutz in den einzelnen Ländern vor, jedoch bestimmt jedes Land den Datenschutz durch seine eigenen Gesetze.

¹⁴³ Vgl. Mayer-Schönberger; Cukier, 2013. S. 241

¹⁴⁴ Vgl. Mayer-Schönberger; Cukier, 2013. S. 248

¹⁴⁵ Vgl. Schmale, Wolfgang; Tinnefeld, Marie-Theres (2014): Privatheit im digitalen Zeitalter. Wien: Böhlau Verlag. S. 79

¹⁴⁶ Vgl. Bundeskanzleramt Österreich: Was ist Datenschutz? Abrufbar unter: <https://www.bka.gv.at/site/5808/default.aspx> (22.08.2014)

6.1.2. Datenschutz in Österreich

In Österreich ist der Schutz personenbezogener Daten verfassungsrechtlich als Grundrecht verankert (Datenschutzgesetz 2000).¹⁴⁷ Dort heißt es im Artikel 1 Grundrecht auf Datenschutz, Paragraph 1, Absatz 1 „Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.“¹⁴⁸ Seit Jänner 2014 gibt es in Österreich eine zuständige Behörde für den Datenschutz, die weisungsunabhängige Datenschutzbehörde, welche die Datenschutzkommission ablöst. Ihre Aufgabe ist es, für die Einhaltung des Datenschutzgesetzes zu sorgen.

6.1.3. Datenschutz in Deutschland

In Deutschland handelt es sich beim Datenschutz um das Recht der informellen Selbstbestimmung. „Nicht die Daten selbst, sondern die Rechte des von den Daten Betroffenen sind der eigentliche Schutzgegenstand“, schreibt Guido Hobert.¹⁴⁹ Er erklärt, dass der Datenschutz „das Persönlichkeitsrecht des Einzelnen vor einer Beeinträchtigung durch Umgang mit seinen persönlichen Daten schützen [soll].“¹⁵⁰ D.h. die Daten sind nicht vor Zerstörung oder Veränderung geschützt, sondern vor unbefugtem Zugriff, unerlaubter Kenntnisnahme, Verarbeitung oder Nutzung.¹⁵¹ Das deutsche Bundesverfassungsgericht legt mit dem Volkszählungsgesetz (BVerfGE 65, 1) wesentliche Vorschriften für die Erhebung, Verwendung und Übermittlung personenbezogener Daten fest.¹⁵² Wolfgang Schmale und Marie-Theres Tinnefeld schreiben dazu, dass mit diesem Gesetz die Bürger auch wissen können, „wer was wann und bei welcher Gelegenheit über sie weiß“¹⁵³.

¹⁴⁷ Vgl. Bundeskanzleramt Österreich.

¹⁴⁸ Bundesgesetz über den Schutz personenbezogener Daten. Datenschutzgesetz 2000 – DSG 2000. Artikel 1, § 1, (1). Abrufbar unter: <http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597> (24.04.2014)

¹⁴⁹ Hobert, Guido (2000): Datenschutz und Datensicherheit im Internet. Interdependenz und Korrelation von rechtlichen Grundlagen und technischen Möglichkeiten. 2., durchgesehene Auflage. Frankfurt am Main: Peter Lang Verlag. S. 80

¹⁵⁰ Hobert, 2000. S. 80f.

¹⁵¹ Vgl. Hobert, 2000. S. 81

¹⁵² Vgl. BVerfGE, 65, 1

¹⁵³ BVerfGE 65, I (42). Siehe auch: Schmale, Wolfgang; Tinnefeld, Marie-Theres, 2014. S. 81

6.1.4. Datenschutz in Italien

Ebenso gilt in Italien der Schutz der persönlichen Daten als Grundrecht eines jeden Individuums. Dank dieses Rechtes kann jeder seine persönlichen Daten schützen und die Verwendung durch Dritte darf nur im Rahmen der Gesetze durchgeführt werden.¹⁵⁴ Das Recht beinhaltet u.a. das Recht auf Auskunft über die eigenen Daten, der Aktualisierung, Berichtigung und Löschung, sowie das Widersprechen zur Verarbeitung von persönlichen Daten.¹⁵⁵

6.1.5. Datenschutz in der EU

In der EU ist der Schutz personenbezogener Daten in Artikel 8 der EU-Grundrechtcharta als Grundrecht verankert.¹⁵⁶ Eine Vereinheitlichung des Datenschutzes auf der Ebene der Europäischen Union erfolgte mit der Richtlinie des europäischen Parlaments und des Rates vom 24.10.1995 (RL 95/46/EG, „Datenschutzrichtlinie“). Die supranationale Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr gewährleistet einen Mindeststandard an Datenschutz in allen Mitgliedsstaaten.¹⁵⁷ Im Jahr 2002 wurde diese Richtlinie im Bereich elektronische Kommunikation mit der Richtlinie 2002/58/EG ergänzt.¹⁵⁸ Die Richtlinie von 2006 (RL 2006/24/EG) über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EC, wurde vom Europäischen Gerichtshof am 8. April 2014 für ungültig erklärt.¹⁵⁹ Sie muss nun überarbeitet werden. Darüber hinaus gibt es weitere Rechtsakten auf europäischer

¹⁵⁴ Vgl. Garante per la protezione dei dati personali: Cosa è il diritto alla protezione dei dati personali? Abrufbar unter: [http://www.garanteprivacy.it/web/guest/home/diritti/cosa-%C3%A8-il-diritto-alla-protezione-dei-dati-personali?*](http://www.garanteprivacy.it/web/guest/home/diritti/cosa-%C3%A8-il-diritto-alla-protezione-dei-dati-personali?) (27.08.2014)

¹⁵⁵ Vgl. Garante per la protezione dei dati personali.

¹⁵⁶ Vgl. Europäische Kommission (25.01.2012): Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Brüssel. Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF> (24.04.2014)

¹⁵⁷ Vgl. Hobert, 2000. S. 92

¹⁵⁸ Vgl. Amtsblatt der Europäischen Gemeinschaft (31.07.2002): Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verwendung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation). Abrufbar unter: <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&qid=1421060648973&from=DE> (15.09.2014)

¹⁵⁹ Vgl. Urteil des Gerichtshofes (Große Kammer) (8. April 2014). Abrufbar unter: <http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d2dc30d69f3cd7a602ad4afda4efdf80276db4a4.e34KaxiLc3qMb40Rch0SaxuOb3f0?text=&docid=150642&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=112813> (15.09.2014)

Ebene, wie etwa die Verordnung über Datenschutz bei der Datenverarbeitung durch Organe und Einrichtungen der Gemeinschaft (Vo Nr. 45/2001) oder die Datenschutzkonvention des Europarates (ETS 108) samt Zusatzprotokoll,¹⁶⁰ welche als internationales Abkommen Staaten weltweit offen steht und für jene Staaten, die sie ratifiziert haben auch verbindlichen Charakter hat.

6.1.6. Datenschutzabkommen zwischen Europa und den USA

In den USA wird der Datenschutz im Gegensatz zu der EU anders gehandhabt. Die Vereinigten Staaten „verwenden einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und Selbstregulierung basiert“.¹⁶¹ Gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, hinsichtlich des Artikel 25, Absatz 6, ergeben sich Einschränkungen für den Datentransfer von EU-Mitgliedsstaaten in Drittländer. Die Übermittlung von personenbezogenen Daten aus EU-Mitgliedsstaaten in nicht EU-Länder ist nur dann zulässig, wenn im Drittland ein angemessenes Schutzniveau sichergestellt werden kann.¹⁶² Dies war laut Europäischer Kommission bei den Vereinigten Staaten nicht der Fall. Weil viele Firmen gerade in den USA ihren Sitz haben und enge Handelsbeziehungen mit Europa bestehen, wurde im Jahr 2000 das Safe-Harbor-System geschaffen, welches einen ausreichenden Schutz für die Übermittlung und Verarbeitung von personenbezogenen Daten aus der Gemeinschaft an US-Unternehmen garantiert. Diese Entscheidung der Europäischen Kommission zusammen mit dem Handelsministerium der USA ermöglicht es US-Unternehmen, sich den „Grundsätzen des sicheren Hafens“ und den dazugehörigen, verbindlichen „Häufig gestellten Fragen“ (FAQ) zu verpflichten und somit die Erlaubnis für die Verarbeitung von personenbezogenen Daten aus der EU zu erhalten.¹⁶³

6.1.7. Das Verhältnis von Big Data und Datenschutz

Im Zuge der Big Data Analysen und der vielfachen Wiederverwendung von Daten für Zwecke, für deren Verwendung bei der Datenerhebung jedoch keine Zustimmung erteilt wurde, öffnet sich hier ein großes Problem für den Datenschutz. Wenn zum Zeitpunkt der

¹⁶⁰ Vgl. Bundeskanzleramt Österreich: Was ist Datenschutz?

¹⁶¹ Entscheidung der Kommission vom 26. Juli 2000. Amtsblatt der Europäischen Union. K(2000) 2441. Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF> (29.08.2014)

¹⁶² Vgl. Entscheidung der Kommission vom 26. Juli 2000.

¹⁶³ Vgl. Entscheidung der Kommission vom 26. Juli 2000..

Datenerhebung der spätere Verwendungszweck noch gar nicht bekannt ist, „ist das vertraute Mittel der Einverständniserklärung oftmals entweder zu restriktiv, um Daten wiederverwenden zu können, oder zu machtlos, um die Privatsphäre des Einzelnen zu schützen.“¹⁶⁴ Deshalb stellen sich Mayer-Schönberger und Cukier, in Anlehnung an das mehrjährige Projekt des Center for Information Policy Leadership über die Wechselwirkung von Haftung und Datenschutz, einen ganz anderen gesetzlichen Datenschutzrahmen vor.¹⁶⁵ Dieser sollte anstelle der Zustimmung bei der Datenerhebung des Einzelnen, die Nutzer der Daten in die Verantwortung nehmen, sodass diese den neuen Verwendungszweck der personenbezogenen Daten förmlich prüfen, besonders im Hinblick auf die Auswirkungen auf die betroffenen Personen.¹⁶⁶ Die Autoren sind überzeugt, dass die Datenschutzgesetzte künftig grobe Verwendungskategorien vorgeben, womit eine Datennutzung ohne oder mit begrenzten, standardisierten Schutzmaßnahmen zugelassen wird.¹⁶⁷ Der Vorteil liegt dabei in der Möglichkeit der kreativen Wiederverwendung der Daten und im gleichzeitigen Schutz für die Daten der Betroffenen. Für mangelnde oder schlampige Datenschutzprüfungen würde somit der Datennutzer rechtlich bestraft werden.¹⁶⁸ Aber auch der Einsatz innovativer Technik kann in bestimmten Fällen den Datenschutz gewährleisten, beispielsweise mit der „differential privacy“, bei der die Daten absichtlich „unscharf“, also nur mit Näherungswerten, dargelegt werden und somit eine exakte Zurückverfolgung konkreter Personen unmöglich wird.¹⁶⁹

6.2. Die Datensicherheit

Hobert schreibt dazu: „Die Datensicherheit umfaßt (sic!) diejenigen Maßnahmen, die erforderlich sind, um gespeicherte Daten vor unbefugten Zugriff und Zerstörung zu schützen.“¹⁷⁰ Sie beinhaltet die Wahrung der Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Daten.¹⁷¹ Durch die Verordnung (EG) Nr 45/2001 des

¹⁶⁴ Mayer-Schönberger; Cukier, 2013. S. 194

¹⁶⁵ Siehe dazu: Bruening, Paula J. (06/ 2012): Interoperability: analysing the current trends & developments. Data Protection Law& Policy. Issue 100.

(http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/DPLP_Interoperability_Bruening.pdf) (26.06.2014)

¹⁶⁶ Vgl. Mayer-Schönberger; Cukier, 2013. S. 217f.

¹⁶⁷ Vgl. Hobert, 2000. S. 218

¹⁶⁸ Vgl. Hobert, 2000. S. 218

¹⁶⁹ Vgl. Hobert, 2000. S. 220

¹⁷⁰ Hobert, 2000. S. 81

¹⁷¹ Vgl. Hobert, 2000. S. 81

Europäischen Parlaments und des Rates regelt die Europäische Gemeinschaft die Sicherheit der Verarbeitung von Daten. Gemäß Artikel 22 „hat der für die Verarbeitung Verantwortliche technische und organisatorische Maßnahmen zu treffen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.“¹⁷²

6.3. Die Berührungspunkte von Datenschutz und Datensicherheit¹⁷³

Obwohl Datenschutz und Datensicherheit oft in einem Atemzug genannt werden, haben sich die Begriffe unabhängig voneinander entwickelt, weisen unterschiedliche Bedrohungspotentiale auf und haben teilweise verschiedene Zielrichtungen. „Es gibt jedoch auch Punkte, an denen sich Datenschutz und Datensicherheit überschneiden. [...] Vereinfachend gesagt fällt dem Datenschutz der rechtliche und der Datensicherheit der technische Aspekt der Problemlösung zu.“¹⁷⁴

6.4. Begriffsdefinition: Daten im Sinne des Datenschutzes

Im Sinne des Datenschutzes versteht man unter dem Begriff Daten generelle Informationen über eine bestimmte Person, womit ihr Name, das Geburtsdatum und die Adresse, aber auch zum Beispiel Stimm aufnehmen, sowie biometrische Daten, wie Bilder und Fingerabdrücke, gemeint sind.¹⁷⁵ Daten können Angaben über Personen enthalten und sind je nach der Intensität des Personenbezuges zu unterscheiden in direkt personenbezogene Daten, mit denen die Identität einer Person bestimmt oder bestimmbar ist, indirekt personenbezogene Daten, bei denen der Empfänger der Daten mit rechtlich zulässigen Mitteln die Person nicht bestimmen kann und nicht personenbezogene (anonymisierte) Daten, die unter keinen Umständen auf den Betroffenen zurückführbar sind. Bei den letzten beiden Datenarten sind sich Big Data-Experten uneinig, ob diese Daten, bei einer genügend großen Datenmenge wohl nicht doch auf die anonyme Person zurückverfolgbar sind. Zudem können Daten nach ihrem Grad der Schutzwürdigkeit

¹⁷² Amtsblatt der Europäischen Gemeinschaft (12.01.2001): Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr. Abrufbar unter: <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32001R0045&from=DE> (15.09.2014)

¹⁷³ Vgl. Hobert, 2000. S. 82

¹⁷⁴ Hobert, 2000. S. 82

¹⁷⁵ Bundeskanzleramt Österreich: Was ist Datenschutz?

unterteilt werden in sensible Daten, welche besonders schutzwürdig sind, und nicht sensible Daten. Zu den sensiblen Daten zählen die rassische und ethnische Herkunft, die politische Meinung, die Gewerkschaftszugehörigkeit, die religiöse oder philosophische Überzeugung, die Gesundheit oder das Sexualleben.¹⁷⁶

6.5. Die Verwendung von Daten

In Österreich ist es als Grundrecht verankert, dass jede Person ein Recht auf die Geheimhaltung ihrer Daten hat. Dieses kann jedoch unter bestimmten Bedingungen rechtmäßig eingeschränkt werden und Daten können von anderen als der betroffenen Person verarbeitet und übermittelt werden. Dies ist der Fall, so das Bundeskanzleramt Österreich, wenn „die Verwendung der Daten im lebenswichtigen Interesse des Betroffenen, mit seiner Zustimmung oder zur Wahrung überwiegender berechtigter Interessen eines anderen (hierzu zählt auch ein öffentliches Interesse) erfolgt.“¹⁷⁷

Die geregelte Verwendung ist wichtig, weil natürlich auch bei der Benützung eines Smartphones und der dazugehörigen Dienstleistungen (App's) stets die Zustimmung für die Verwendung der eigenen Daten erteilt werden muss. Diese Einwilligung kann jederzeit zurückgenommen werden. Jedoch warnt die EU-Initiative für mehr Sicherheit im Netz, klicksafe.de, dass verschiedene Apps teils auch ohne Einwilligung des Nutzers auf Daten zugreifen, die für das Funktionieren der App nicht zwingend notwendig sind.¹⁷⁸

Dazu gehören z.B. der Zugriff auf das Adressbuch des Nutzers, aber auch alle anderen gespeicherten Daten auf dem Smartphone können davon betroffen sein. Riskant wird die unerlaubte Einsicht in gespeicherte Daten, wenn es sich dabei um TANs fürs Online Banking oder um Kreditkarteninformationen handelt. Die EU-Initiative rät daher zu einer gesunden, kritischen Haltung gegenüber Apps, einer genauen Prüfung der Allgemeinen Geschäftsbedingungen und Kontrolle, welche Zugriffsrechte sich die App einräumen möchte.¹⁷⁹

¹⁷⁶ Vgl. Bundeskanzleramt Rechtsinformationssystem (RIS): Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutzgesetz 2000, Fassung vom 22.08.2014. DSG 2000, Art. 2 § 4 z 1,2. Abrufbar unter:

<https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597> (22.08.2014)

¹⁷⁷ Bundeskanzleramt Österreich: Was ist Datenschutz? Abrufbar unter:

<https://www.bka.gv.at/site/5808/default.aspx> (22.08.2014)

¹⁷⁸ Vgl. EU-Initiative für mehr Sicherheit im Netz. Apps & Datenschutz. Abrufbar unter:

<http://www.klicksafe.de/themen/kommunizieren/smartphones/apps-datenschutz/> (27.08.2014)

¹⁷⁹ Vgl. EU-Initiative für mehr Sicherheit im Netz.

6.6. Die Vorratsdatenspeicherung

Unter der Vorratsdatenspeicherung versteht man die Speicherung von personenbezogenen Daten durch öffentliche Stellen, ohne dass die Daten aktuell benötigt werden. Die Richtlinie des Europäischen Parlament und des Rat von 2006 2006/24/EG, sah die Vorratsspeicherung von Daten vor, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet wurden. Die sehr umstrittene Richtlinie regelte, dass Anbieter von Telekommunikationsdiensten Verbindungsdaten auf Vorrat speicherten.

Der Europäische Gerichtshof urteilte jedoch am 8. April 2014, dass die Speicherung von Kommunikationsdaten ohne Verdacht auf Straftaten nicht mit dem EU-Gesetz vereinbar ist und betonte, dass die Richtlinie „einen besonders schwerwiegenden Eingriff [...] in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten“¹⁸⁰ darstellt. Die EU-Kommission muss die Vorschriften zur Vorratsdatenspeicherung nun überarbeiten.

6.7. Die Überwachung der Telekommunikation heute

Die Handy-Überwachung hat weltweit nahezu inflationäre Ausmaße angenommen, von denen kaum jemand etwas weiß.¹⁸¹ Auch wenn die Vorratsdatenspeicherung derzeit nicht erlaubt ist, so sind nicht nur staatliche Mächte an unseren Daten interessiert. Sicher scheint, dass die Überwachung auch für wirtschaftliche Zwecke genutzt wird, was umso erschreckender ist. Wie Stefan Heuer und Pernille Tranberg zu Recht sagen, sind Handys heutzutage keine Telefone mehr, sondern tragbare Hochleistungsrechner, die immer mehr und immer intelligentere Dienstleistungen anbieten.¹⁸² Mit Hilfe der Smartphones werden wir zu gläsernen Bürgern und Verbrauchern, darin sind sich Wissenschaftler und Experten einig. Denn neben Mobilfunkbetreibern und Geheimdiensten, speichern auch App-Anbieter oder dergl. nicht nur Telekommunikationsdaten, sondern kopieren sich auch höchst private Daten von unserem Handy auf ihren Rechner.¹⁸³ Beispiele bei denen

¹⁸⁰ Gerichtshof der Europäischen Union: Pressemitteilung Nr. 54/14. Luxemburg, den 8. April 2014. Abrufbar unter: <http://malte-spitz.de/wp-content/uploads/2014/04/CP140054DE.pdf> (25.08.2014)

Vgl. auch : Urteil des Europäischen Greichtshof. 08. April 2014. Abrufbar unter: http://curia.europa.eu/juris/document/document_print.jsf?doclang=DE&text=&pageIndex=0&part=1&mode=req&docid=150642&occ=first&dir=&cid=316886#Footnote* (25.08.2014)

¹⁸¹ Vgl. Kotteder, Franz (2011): Die wissen alles über Sie. Wie Staat und Wirtschaft Ihre Daten ausspionieren – und wie Sie sich davor schützen. 1. Auflage. München: Redline Verlag. S. 120f.

¹⁸² Vgl. Heuer; Tranberg, 2013. S. 59

¹⁸³ Vgl. Kotteder, 2011. S. 120, sowie: vgl. Heuer; Tranberg, 2013. S. 59

durch die Installation von Dienstleistungen (Apps) ganze Adressbücher, Fotoalben, Textnachrichten, Kalendernotizen, Standortdaten, auch bei ausgeschalteter Standortsuche, sowie weitere Informationen vom Handy der Nutzer auf die Server der jeweiligen Unternehmen geladen wurden, gibt es zuhauf.¹⁸⁴ All dies passiert häufig ohne das Wissen der Nutzer.¹⁸⁵ Laut der Sicherheitsfirma Bitdefender, die im Sommer 2012 65.000 der beliebtesten Apps auf ihr „Verhalten“ kontrollierte, verfolgten 41 Prozent der untersuchten Apps die Standorte der Benutzer, 33 Prozent speicherten die Nutzerinformationen ohne Verschlüsselung, 18,6 Prozent hatten Zugriff auf alle Kontaktdaten im Adressbuch und 16,4 Prozent konnten sich mit Facebook verbinden.¹⁸⁶ Häufig ist es jedoch auch so, dass App-Anbieter die Zustimmung der Nutzer für die diverse Verwendung ihrer Daten erhalten, da Nutzer den Nutzungs- und Datenschutzbedingungen bereitwillig zustimmen.

Auch kostenlose WLAN-Verbindungen empfehlen die Autoren zu meiden, denn es bedarf nur minimales Fachwissen oder die richtigen Spionagesoftwares um in die persönlichen Daten anderer Nutzer im offenen, drahtlosen Netzwerk, sowie deren Passwörter einzusehen.¹⁸⁷

6.8. Der Datenschutz am eigenen Smartphone

Ob Verbindungsdaten von Netzbetreibern gespeichert werden (z.B. Daten bei Telefonaten, SMS, Internetzugang), können Smartphone-Nutzer nicht am eigenen Smartphone einstellen. Jedoch können sie die Daten, die sie am Handy speichern, wie z.B. Fotos, Adressbücher, Notizen, etc. schützen. Die EU-Initiative für mehr Sicherheit im Netz, verweist dabei zum einen auf das aufmerksame Durchlesen der

1. ¹⁸⁴ Siehe dazu als Beispiel:

2. Chen, Brixian X. (01.02.2013): Privacy Flaw in Path's iPhone App Shares Location Data. The New York Times. Bits. 16:11 Uhr. Abrufbar unter: <http://bits.blogs.nytimes.com/2013/02/01/path-photos-location-loophole/> (27.06.2014)

Perlroth, Nicole (05.06.2012): LinkedIn's Leaky Mobile App Has Access to Your Meeting Notes. The New York Times. Bits. 20:00 Uhr. Abrufbar unter: <http://bits.blogs.nytimes.com/2012/06/05/linkedins-leaky-mobile-app-has-access-to-your-meeting-notes/> (27.06.2014)

Sowie weitere Beispiele: Vgl. Heuer; Tranberg, 2013 60ff.

¹⁸⁵ Siehe als Beispiel: Dingers, Gary (13.03.2012): Lawsuit: Mobile apps accessing users' address books. Statesman. Abrufbar unter: <http://www.statesman.com/news/business/lawsuit-mobile-apps-accessing-users-address-books/nRmCT/> (27.06.2014)

¹⁸⁶ Vgl. Rowinski, Dan (20.07.2012): Apple won't let you see what iPhone Apps do with your data. ReadWrite. Abrufbar unter: <http://readwrite.com/2012/07/20/apple-wont-let-you-see-what-iphone-apps-do-with-your-data#feed=/search?keyword=apple+wont+let+you+see+what+iphone+apps+do+whit+your+data&awesm=~oInqbRkKqxRJVS> (27.06.2014)

¹⁸⁷ Vgl. Heuer; Tranberg, 2013. S. 66

Datenschutzrichtlinien beim Herunterladen und/oder Installieren einer App, weil dort meistens auch die Berechtigungen aufgelistet sind, welche sich die App verschaffen möchte. Zum anderen können auch Einstellungen direkt am Smartphone für mehr Sicherheit sorgen. Dazu gehört das nachträgliche Überprüfen der Anwendungen und deren Berechtigungen, der Deaktivierung von Hintergrunddaten, welche die jederzeit automatische Aktualisierung, sowie das Senden und Empfangen von Daten unterbindet, der Überprüfung des Verbrauchs von Akku, Rechenzeit und Datentransfer. Bei erhöhtem Verbrauch nach der Installation einer App sollte diese entfernt werden, weil diese möglicherweise ungewollt Daten über das Smartphone aussendet. Zu einer Vorsichtsmaßnahme gehört auch bei Updates von Apps das erneute Überprüfen der Datenschutzrichtlinie und der Berechtigung. Oft ändern Anbieter diese Bestimmungen, weswegen es sich empfiehlt, Updates immer manuell durchzuführen.¹⁸⁸

7. Das Post-Privacy- Zeitalter

7.1. Begriffsdefinition

Es hat eine neue Zeitrechnung begonnen, nach dem Zeitalter der Privatsphäre leben wir heute im „Post-Privacy-Zeitalter“.¹⁸⁹ Gemeint ist damit der Zustand einer immer kleiner werdenden Privatsphäre bis hin zur totalen Öffentlichkeit und Transparenz. Ermöglicht und gefördert wird diese Entwicklung durch das Internet, welches es uns ermöglicht, Informationen in großem Ausmaß preiszugeben und weltweit auszutauschen. Eine vollendete Post-Privacy wirft alles über jeden in ein gemeinsames, öffentliches Forum. Sie verweigert Selbstzensur¹⁹⁰ und „verbannt Privates nicht in die dafür vorgesehenen Räume, sondern stellt es gleichberechtigt mit allem anderen in die Öffentlichkeit“.¹⁹¹

7.2. Die Möglichkeiten des Data Mining

Dass wir diesem Zeitalter bereits nahe sind, zeigt Big Data mit der Möglichkeit auf, aus den von uns eingegebenen Daten, Informationen zu generieren, die wir in keinsten Weise veröffentlicht oder auch nur eingegeben haben. Die Privatsphäre hört im Internet nämlich

¹⁸⁸ Vgl. EU-Initiative für mehr Sicherheit im Netz.

¹⁸⁹ Vgl. Koidl, 2013. S. 55

¹⁹⁰ Vgl. Heller, Christian (2011): Post-Privacy. Prima leben ohne Privatsphäre. München: Verlag C.H.Beck. S. 140

¹⁹¹ Heller, 2011. S. 140

nicht erst dort auf, wo man ausdrücklich etwas mitteilt.¹⁹² Durch die Analyse von selbst eingegebenen Daten können, vorausgesetzt es sind genügend Datenmengen und Statistiken verfügbar, diverse Muster erkannt werden.¹⁹³ Mit Hilfe von „Data Mining“ weiß die Denkmachine Internet gelegentlich mehr über uns, als wir selbst, unsere Familie und Freunde zusammen. Was wir dem System nicht direkt mitteilen, erfasst und folgert es selbst – notfalls auch ohne unsere Erlaubnis.¹⁹⁴ An diesem Punkt versuchen auch der Datenschutz und die „informationelle Selbstbestimmung“ einzuhaken, mit der Forderung, Datenströme kontrollierbar zu machen. Daten sollen so verwendet werden, wie der „Besitzer“ es anordnet.¹⁹⁵

7.3. Machtverhältnis – Der Kontrollverlust unserer Daten

Der Kontrollverlust unserer Daten zeigt ein Machtverhältnis auf, denn Wissen über uns kann auch als Machtmittel gegen uns verwendet werden. „Macht ist die Fähigkeit, Menschen, Dinge, Verhältnisse in eine bestimmte Richtung zu drängen, zu beeinflussen, zu formen.“¹⁹⁶ Macht funktioniert aber vor allem durch die Verhinderung von Wissen. Wenn Menschen nicht wissen, wann sie überwacht werden und wann nicht, macht dies die Überwachung allgegenwärtig und die Menschen somit gefügig. Datenschützer pochen daher auf den Auskunftsanspruch eines Jeden über das Ausmaß und die Benützung seiner Daten durch andere.¹⁹⁷

7.4. Vor- und Nachteile eines Lebens ohne Privatsphäre

Ein Vorteil von Post-Privacy ist die Möglichkeit in Situationen, in denen man sich allein fühlt, Gleichgesinnte zu finden. Die Kehrseite der Medaille ist dabei, dass auch umso leichter Andersheit identifiziert werden kann und diese auch sehr gezielt bekämpft werden kann.¹⁹⁸

Zu Post-Privacy finden kontroverse Argumentationen statt. Christian Heller sieht die Entwicklung als unaufhaltbar, und verweist somit auf die Vorteile, die uns aus totaler Transparenz erwarten. Dabei nennt er beispielsweise das „Ugol’sche Gesetz“, das Wissen

¹⁹² Vgl. Heller, 2011. S. 12

¹⁹³ Vgl. Heller, 2011. S. 13

¹⁹⁴ Vgl. Heller, 2011. S. 15

¹⁹⁵ Vgl. Heller, 2011. S. 84f. Vgl. dazu auch: Schmale, Wolfgang.; Tinnefeld, Marie-Theres, 2014. S. 33

¹⁹⁶ Heller, 2011. S. 95

¹⁹⁷ Vgl. Heller, 2011. S. 100

¹⁹⁸ Vgl. Heller, 2011. S. 142

in jeglichen, auch noch so ausgefallenen Verhaltensweisen, Einstellungen, Werthaltungen nicht der Einzige zu sein.¹⁹⁹ Um mit der Offenlegung sämtlicher Lebensdetails anderer zurechtzukommen, rät er zur „Filtersouveränität“, d.h. nur dem Beachtung zu schenken, was wir auch wirklich wissen wollen - alles andere sollen wir ausblenden.²⁰⁰ Laut Marie-Theres Tinnefeld, Benedikt Buchner und Thomas Petri widersprechen dem allerdings soziologische und sozialpsychologische Untersuchungsergebnisse. Sie verweisen darauf, dass der Einzelne eine Wahl haben muss, sich mitzuteilen, oder sich zu verbergen, ansonsten wäre ein Zusammenleben in einer Gesellschaft nicht möglich.²⁰¹ Constanze Kurz und Frank Rieger sehen es als geistigen Kurzschluss, nach der berechtigten Forderung einer Offenlegung staatlichen Handelns und der Transparenz kommunaler Projekte, auch die Offenheit des Bürgers zu fordern.²⁰² Sie stimmen daher dem Leitmotiv des Chaos Computer Clubs zu, der fordert öffentliche Daten zu nützen, private Daten zu schützen.²⁰³ Auch Wolfgang Schmale und Marie-Theres Tinnefeld sehen die Entwicklung hin zur Post-Privacy kritisch.

Manche behaupten, dass die neue Entwicklung zur Bloßstellung der eigenen Privatheit in Internet und zur Überwachung der Gesellschaft unter dem Banner des Staates aus Sicherheitsgründen, zwar zum Ende der Privatheit, aber nicht zum Ende der individuellen Freiheit führe. Dabei wird vergessen, dass Privatheit ein uraltes kulturelles Vermächtnis ist, ein Quellcode der Freiheit des Einzelnen und der offenen Demokratie.²⁰⁴

7.5. Die Transparenzgesellschaft als Folge der heutigen Informationstechnik

Die Transparenzgesellschaft wie sie Byung-Chul Han bezeichnet, oder die transparente Gesellschaft laut Christian Heller, geht mit der Entwicklung der Post-Privacy einher. Auch sie ist eine Folge der heutigen Informationstechnik, die es ihren Anwendern ermöglicht, ihre Welt immer, überall und in jedem Bereich transparent zu halten.²⁰⁵ Doch die damit gebotene Transparenz ist derzeit noch stark asymmetrisch, denn sie kommt

¹⁹⁹ Vgl. Heller, 2011. S. 129 f.

²⁰⁰ Vgl. Heller, 2011. S. 140

²⁰¹ Tinnefeld, Marie-Theres; Buchner, Benedikt; Petri, Thomas (2012): Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht. 5. Auflage. München. S. 52 f.

²⁰² Kurz; Rieger, 2011. S. 184

²⁰³ Vgl. Chaos Computer Club e. V.: Hackerethik. Abrufbar unter: <http://www.ccc.de/de/hackerethik> (28.05.2014)

²⁰⁴ Schmale; Tinnefeld, 2014. S. 11

²⁰⁵ Vgl. Rihaczek, Karl (03/2014): Transparenz. Datenschutz und Datensicherheit –DuD. 38 (3). S. 145. Abrufbar unter: http://download.springer.com/static/pdf/864/art%253A10.1007%252Fs11623-014-0063-3.pdf?auth66=1398438436_b0fe6fc9dcca00e3ee0ce066ca93a8&ext=.pdf (24.04.2014)

vorwiegend nur einer Seite zugute, dem „Oben“. Heller spricht in diesem Zusammenhang von einer vertikal verlaufenden Transparenz.²⁰⁶ Auch wenn dieser Sachverhalt spätestens durch die NSA-Ausspähaffäre angeprangert wird, so ändert er nichts an dem Verhalten der Anwender, die ihre Gewohnheiten, Vorlieben und Aufenthaltsorte weiterhin breitwillig und mit Lust anbieten.²⁰⁷

Byung-Chul Han definiert Transparenz als komplette Durchleuchtung, eine Kontrolle von jedem über jeden, aus allen Perspektiven.²⁰⁸ Garantiert wird diese Transparenz durch die Hyperkommunikation eines jeden einzelnen, der sich nicht aus Zwang der Kontrollgesellschaft beugt, sondern aus freiem Willen, aus einem selbstgenerierten Bedürfnis heraus entblößt, seine Privat- und Intimsphäre aufgibt und schamlos zur Schau stellt.²⁰⁹ Dabei kontrolliert aber nicht nur das Oben das Unten, sondern jeder kontrolliert jeden, welches der Vorstellung einer horizontalen Transparenz nach Heller entspricht. Doch auch in der Transparenzgesellschaft spricht sich Han für den Schutz der eigenen Daten aus. Nicht nur um Sicherheit zu erlangen, was mit den eigenen Daten geschieht, sondern insbesondere, weil die menschliche Seele Bereiche braucht „in denen sie bei sich sein kann ohne den Blick der Anderen. [...] Eine totale Ausleuchte würde sie ausbrennen und eine besondere Art seelischen Burnouts hervorrufen.“²¹⁰ Das Leben mit seiner Spontaneität, Ereignishaftigkeit und Freiheit lässt laut ihm keine Transparenz zu. Deshalb beschreibt Han die Forderung nach einer Ideologie der „Post-Privacy“, die im Namen der Transparenz eine totale Preisgabe der Privatsphäre fordert und zu einer durchsichtigen Kommunikation führen soll, als naiv.²¹¹

Han erklärt, dass die permanente Forderung nach Transparenz auf ein fehlendes Vertrauen hinweist. Denn Vertrauen entsteht in einem Zustand zwischen Wissen und Nicht-Wissen. Und auch wenn man vom Gegenüber nicht alles weiß, ist der Aufbau einer positiven Beziehung möglich. Wenn man hingegen im Vorfeld schon alles über den anderen weiß, so erübrigt sich das Vertrauen.²¹² „In einer auf Vertrauen beruhenden Gesellschaft entsteht keine penetrante Forderung nach Transparenz. Die

²⁰⁶ Vgl. Heller, 2011. S. 112

²⁰⁷ Vgl. Rihaczek, 2014. S. 145, sowie DIVISI U-15-Studie, 2014. S. 12, 142

²⁰⁸ Vgl. Han, Byung-Chul: Transparenzgesellschaft. 3. Auflage. Berlin: MSB Verlagsgesellschaft. 2013. S. 74 f.

²⁰⁹ Vgl. Han, 2013. S. 76-77

²¹⁰ Han, 2013. S. 8

²¹¹ Vgl. Han, 2013. S. 8

²¹² Vgl. Han, 2013. S. 78-79

Transparenzgesellschaft ist eine Gesellschaft des Misstrauens und des Verdachts, die aufgrund des schwindenden Vertrauens auf Kontrolle setzt.“²¹³ Dem widerspricht Heller nicht, denn auch er bezeichnet die Transparenz als demokratisches Prinzip, als Kontrolle der Vielen über ihre Herrschaft. Es ist bildhaft eine Umkehrung des Panopticons.²¹⁴ Für ihn hingegen ist die totale Überwachung von Oben unausweichlich. Daher folgt er in seinen Forderungen jenen des futuristischen Amerikaners David Brin, welcher der Überwachung nicht den Kampf ansagt, sondern sie besser demokratisch verteilen möchte. Brins Vorschlag lautet, dass wenn die Überwachung schon total wird, sie für alle zur Verfügung stehen sollte und somit zur gegenseitigen Überwachung wird.²¹⁵ Er vertraut dabei auf den technischen Fortschritt und die Möglichkeit seiner Ausbreitung. Somit würde die totale Überwachung zur totalen Transparenz, denn erst die ungleiche Verteilung der Möglichkeiten zur Überwachung bilden ein Machtmittel.²¹⁶ Wenn also die Privatsphäre durch die totale Demokratisierung der Überwachung ohnehin wegbricht, dann spricht sich Heller klar für das Vorziehen der transparenten Gesellschaft, anstelle des Orwell’schen Panoptismus aus, welcher uns vollkommen und allein einer zentralen Überwachungsgewalt ausliefern würde.²¹⁷

8. Forschungsfragen

Forschungsleitende Frage 1: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über Big Data im Allgemeinen?

Forschungsleitende Frage 2: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über die Datenspeicherung im Zusammenhang mit der Nutzung von Smartphones?

Forschungsleitende Frage 3: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über die Auswertung und Analyse ihrer Daten, die sie bei der Nutzung ihres Smartphones generieren?

²¹³ Han, 2013. S. 79

²¹⁴ Vgl. Heller, 2011. S. 107

²¹⁵ Brin, David (1998): The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom? New York: Perseus Book Group. S. 333-335

²¹⁶ Vgl. Heller, 2011. S. 111 f.

²¹⁷ Vgl. Heller, 2011. S. 119

Forschungsleitende Frage 4: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über die Vorhersagbarkeit ihres Verhaltens im Zusammenhang mit der Nutzung von Smartphones?

Forschungsleitende Frage 5: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über die möglichen Folgen von Big Data in der Zukunft im Zusammenhang mit der Nutzung von Smartphones?

9. Untersuchung

9.1. Forschungsdesign

Das Ziel dieser Arbeit ist es, das Wissen von jungen Erwachsenen im Alter zwischen 18 und 24 Jahren im Hinblick auf Big Data in Verbindung mit der Nutzung von Smartphones zu untersuchen. Das theoretische Konstrukt Wissen wird für diese Arbeit in den Bereichen Fakten- und Strukturwissen unterteilt, um möglichst aussagekräftige Erkenntnisse zu erhalten.

Da bei der Erstellung der Forschungsarbeit nur ein äußerst geringer Prozentsatz der Personen im näheren Umfeld der Autorin, unabhängig ihres Alters, Bildungsgrades, Arbeitssituation, Wohnortes und Nationalität über Big Data Bescheid wusste, wird die Untersuchung mit Hilfe von qualitativen Interviews durchgeführt. Durch das unzureichende Wissen über Big Data in einer ersten Umfrage wird befürchtet, dass eine quantitative Untersuchung mittels Fragebogen nicht aufschlussreich wäre, weil die Untersuchungspersonen die Fragen nicht verstehen könnten und daher möglicherweise nicht antworten, oder eventuell raten würden. Die Untersuchung wird qualitativ mit Hilfe von Leitfadeninterviews durchgeführt. Es handelt sich um eine Fallstudie mit kleinen Stichproben, wobei die Tiefenperspektive der Befragten wichtiger ist als die Vergleichbarkeit der Antworten.²¹⁸

Bei der anschließenden Transkription der Interviews wird in erster Linie auf die Informationen und Inhalte der Antworten geachtet. Die Auswertung der gewonnenen Daten geschieht mit Hilfe einer qualitativen Inhaltsanalyse, welche sich an die qualitative Inhaltsanalyse nach Gläser und Laudel anlehnt. Die Methode der Extraktion mittels Suchraster, welches sich an die theoretischen Vorüberlegungen und Thesen stützt, erwies

²¹⁸ Vgl. Scholl, Armin (2003): Die Befragung. Sozialwissenschaftliche Methode und kommunikationswissenschaftliche Anwendung. Konstanz: UVK Verlagsgesellschaft. S. 67

sich bereits in anderen Untersuchungen als sehr vorteilhaft, da die Informationen nach der Analyse sehr detailliert vorlagen. Das erweist sich auch für die Befragung des Wissens als sehr sinnvoll. Durch die Verwendung des Suchrasters wird eine strukturierte Informationsbasis garantiert, welche im Unterschied zum Ursprungstext ausschließlich jene Informationen beinhaltet, die für die Beantwortung der Forschungsfragen notwendig sind.²¹⁹ Mit Hilfe der Analyseeinheiten wird das Untersuchungsmaterial nachvollziehbar strukturiert. Die Auswertungseinheiten bilden die geführten und transkribierten Interviews. Die Kontexteinheit beinhaltet den größtmöglichen Textbestandteil, der unter eine Kategorie fallen kann, in dieser Arbeit bilden das sinngemäß zusammengehörige Fragen und Antworten. Die Kodiereinheit hingegen setzt sich aus minimalen Textbestandteilen zusammen, worunter einzelne Wörter oder Satzteile verstanden werden.

9.2. Untersuchungsgegenstand

Der Untersuchungsgegenstand ist das Wissen der jungen Erwachsenen im Alter zwischen 18 und 24 Jahren. Für die Untersuchung werden elf Personen interviewt, davon fünf Männer und sechs Frauen. Da die Identität der Untersuchungspersonen bestmöglich geschützt werden möchte, werden nur die notwendigen Informationen der TeilnehmerInnen ohne Zusammenhänge aufgelistet.

Die Untersuchungspersonen werden in drei Altersgruppen aufgeteilt. Zur Altersgruppe 1 gehören die Befragten im Alter zwischen 18 und 20 Jahren, die Altersgruppe 2 umfasst die Befragten im Alter zwischen 21 und 22 Jahren und zur Altersgruppe 3 zählen die Befragten im Alter zwischen 23 bis 24 Jahren. Die TeilnehmerInnen unterscheiden sich durch einen ländlichen (sechs Personen) und städtischen (fünf Personen) Wohnort, Bildungsgrad und Beschäftigung.

Vier UntersuchungsteilnehmerInnen befinden sich derzeit in einer Berufsausbildung, zwei belegen ein Universitätsstudium und fünf Personen sind berufstätig. In der Altersgruppe 1 wurden drei Personen befragt und jeweils vier Personen haben sich in den Gruppen 2 und 3 als Untersuchungspersonen bereit erklärt, an der Untersuchung teilzunehmen.

²¹⁹ Vgl. Gläser, Jochen; Laudel, Grit (2009): Experteninterviews und qualitative Inhaltsanalyse als Instrument rekonstruierender Untersuchung. 3., überarbeitete Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften. S. 200

9.3. Untersuchungsmaterial

Das Untersuchungsmaterial wird mit Hilfe von leitfadengestützten Interviews gewonnen. Die Anzahl der geführten Interviews wurde durch den Informationsgehalt der Antworten bestimmt. Der Umfang der Untersuchungsgruppe beläuft sich auf elf TeilnehmerInnen. Die Interviews wurden persönlich und face-to-face geführt, damit auch die Mimik und Gestik der Interviewten wahrgenommen werden konnte. Da Big Data noch relativ unbekannt ist, konnte somit besser sichergestellt werden, ob der Befragte die Frage auch wirklich verstanden hat oder ob eine genauere Erklärung erforderlich war. Die Interviews wurden einzeln gehalten, wodurch eine bessere Konzentration auf die Informationen gegeben war und das Vertrauen zwischen den Interviewpartnern leichter aufgebaut werden konnte. Damit das Interview bestmöglich einer normalen Gesprächssituation ähnelte und sich die Interviewerin auf das Gespräch konzentrieren konnten, wurde es auf Tonband aufgenommen, was auch den Vorteil mit sich bringt, dass somit alle Informationen für die Auswertung erhalten bleiben.

Das Leitfadeninterview besteht aus den sechs Themenblöcken Big Data, Datenschutz, Datenspeicherung, Datenanalyse, Vorhersagbarkeit des Verhaltens und mögliche Folgen von Big Data mit insgesamt 25 Leitfragen und acht Szenarien. Die Interviews dauerten zwischen 17 und 35 Minuten.

9.4. Transkription

Die Transkription der Interviews erfolgt in der deutschen Standardsprache. Obwohl alle Interviews in deutscher Sprache durchgeführt werden, die Sprache der Untersuchungspersonen aber dialektale Einschläge aufweist, erleichtert die Transkription in der deutschen Standardsprache die anschließende Auswertung und Analyse, sowie das Verständnis für all jene, die bestimmte Dialekte nur schwer oder nicht verstehen.

Da der Informationsgehalt der Antworten erhalten bleiben soll, werden längere Pausen gekennzeichnet, Betonungen oder Akzente werden hingegen nicht gesondert hervorgehoben. Nicht lexikalisierte vokale Äußerungen wie „äh“, „mh“ und dergl., die oft als Pausenfüller verwendet werden, werden nicht transkribiert. Eine Ausnahme bildet die Zustimmungen mit den Äußerungen „Mhm“, sowie die Äußerung des Überlegens „Hm“, welche aufgrund ihres Informationsgehaltes transkribiert werden.

9.5. Untersuchungsmethode

9.5.1. Leitfadeninterview – Vorteile und Kritik

Das Leitfadeninterview bietet sich für diese Untersuchung aufgrund seines geringen Grades an Standardisierung besonders gut an, da im Vorfeld das Wissen des/r Befragten unbekannt ist und durch ein standardisiertes Interview wichtige Informationen nicht erhoben werden könnten. Durch den Leitfaden wird sichergestellt, dass alle relevanten Themen der Untersuchung behandelt werden, die durch die forschungsleitenden Fragen festgelegt sind, und nicht durch die Antworten des/der InterviewpartnerIn bestimmt werden können. Der Vorteil dieser Form der Befragung liegt dabei in der Möglichkeit der variierbaren Reihenfolge der Leitfragen, Hilfestellung bei nicht verstandenen Fragen, und der Möglichkeit bei bestimmten Fragen weiter nachzufragen womit ein umfassenderes Bild des Wissens der Befragten erworben werden kann. Das Leitfadeninterview befindet sich dabei in einem Spannungsfeld zwischen Offenheit und Strukturiertheit, wie es Jan Kruse treffend beschreibt, wobei der Aufbau dem Prinzip folgt: vom Offenen zum Strukturierenden.²²⁰

Der Nachteil des geringen Standardisierungsmaßes liegt darin, dass die Auswertung im Anschluss durch die Breite der Antworten erschwert wird. Ein grundlegendes Problem von Interviews, auf das Jochen Gläser und Grit Laudel aufmerksam machen und auf das auch bei dieser Untersuchung Rücksicht genommen werden muss, ist die unterschiedliche Sprache mit der sich die InterviewpartnerInnen begegnen. Das Erkenntnisinteresse der Interviewerin, sowie die Interviewfragen entstehen aus einem wissenschaftlichen Kontext heraus, wodurch auch die Sprache eine wissenschaftliche ist. Im Gegensatz dazu kann sich die Sprache des/r Befragten in seiner/ihrer Lebenswelt deutlich unterscheiden. So kann es zwar sein, dass der/die Befragte Fachbegriffe begreift, aber ihnen eine andere Bedeutung zuschreibt, ohne dass das im Interview deutlich wird und seine/ihre Antworten somit von der Interviewerin anders verstanden werden, als sie gemeint waren.²²¹ Die Interviewfragen müssen daher an den kulturellen Kontext der Befragten angepasst werden. „Diese Operationalisierung beginnt bei der Formulierung von Leitfragen [...], wird bei der Entwicklung des Leitfadens fortgesetzt und muss im Interview spontan

²²⁰ Vgl. Kruse, Jan (2014): Qualitative Interviewforschung. Ein integrativer Ansatz. Weinheim und Basel: Beltz Juventa. S. 207, 213, 218

²²¹ Vgl. Gläser; Laudel, 2009. S. 112f.

bewältigt werden.“²²² Das qualitative Interview ist deshalb eine permanente, spontane Operationalisierung.

9.5.1.1. Interviewfragen

Die Interviewfragen werden im Leitfaden, der als Instrument der Datenerhebung dient, auch als Gerüst für den Gesprächsverlauf verstanden. Die offenen Fragen unterliegen den wissenschaftlichen Kriterien und erfüllen die wichtigsten Anforderungen der Klarheit, Einfachheit und Verständlichkeit. Mit Hilfe der sechs Fragenblöcke zu den Themen Big Data, Datenschutz, Datenspeicherung, Datensammlung, Vorhersagbarkeit der Zukunft und mögliche Folgen von Big Data, werden diese abgehandelt und erörtert. Aufgrund einer besseren Verständlichkeit werden manche Fragen nicht direkt gestellt, sondern als Szenarien einer möglichen Big Data-Zukunft geschildert und die UntersuchungsteilnehmerInnen anschließend gefragt, ob sie das für möglich bzw. für realistisch halten oder nicht. Mit Hilfe der Big Data Zukunftsszenarien wird die Aktivierung des latenten Wissens angestrebt, sodass dies externalisiert werden kann. Die InterviewpartnerInnen sind sich bereits bekannt, deshalb wird das höfliche Du verwendet.

9.5.2. Qualitative Inhaltsanalyse – Vorteile und Kritik

Die Methode der qualitativen Inhaltsanalyse bietet sich für diese Untersuchung besonders gut an, weil sie die Aufdeckung der relevanten Einzelfaktoren für die jeweiligen Themen ermöglicht und gleichzeitig die Konstruktion von möglichen Zusammenhängen dieser Faktoren erleichtert.²²³ „Das Material wird immer in seinem Kommunikationszusammenhang verstanden (...) [und] somit immer innerhalb eines Kontextes interpretiert (...) [und] auch auf seine Entstehung und Wirkung hin untersucht“.²²⁴ Gläasers und Laudels Model der qualitativen Inhaltsanalyse eignet sich in diesem Fall besonders gut, weil sie mit der Extraktion der Daten arbeitet. Bei der Extraktion werden dem Text für die Untersuchung relevante Informationen entnommen und in die entsprechenden Kategorien des Suchrasters eingetragen und somit gleich strukturiert.²²⁵ Einen weiteren Vorteil der qualitativen Inhaltsanalyse nach Gläser und

²²² Gläser; Laudel, 2009. S. 112

²²³ Vgl. Mayring, Philipp (2007): Qualitative Inhaltsanalyse. Grundlagen und Techniken. 9. Auflage. Weinheim: Beltz Verlag. S. 20

²²⁴ Mayring, 2007. S. 42

²²⁵ Vgl. Gläser; Laudel, 2009. S. 200

Laudel im Vergleich zu jener von Mayring bietet die Tatsache, dass das Kategoriensystem auch während der Untersuchung um Faktoren erweitert werden darf, wobei darauf zu achten ist, dass die bereits zugefügten Textteile immer noch der Kategorie entsprechen.²²⁶ Der Vorteil der Offenheit der Kategorien bringt jedoch auch den Nachteil mit sich, dass sich die Kategorien schwer auf gezielte Informationen beschränken lassen.

Die qualitative Inhaltsanalyse wird in vier Schritten durchgeführt:

1. Entwicklung des Suchrasters
2. Extraktion der Inhalte
3. Aufbereitung der Inhalte
4. Auswertung der Inhalte

9.6. Kategoriensystem

Die Entwicklung des Suchrasters erfolgte in Anlehnung an die forschungsleitenden Fragen. Es beinhaltet neben den Kategorien zu den sechs Themenschwerpunkten aber auch die Kategorien Medienkonsum und Smartphonegebrauch. Durch das kommunikationswissenschaftliche Interesse dieser Arbeit ist es ausschlaggebend, die Mediennutzungsgewohnheiten der Untersuchungspersonen zu kennen. Die Kategorien bilden sich wie folgt:

Kategorie 1: Medienkonsum

Kategorie 2: Smartphonegebrauch

Kategorie 3: Wissen über Big Data

Big Data als Begriff

Bedeutung von „Big Data“

Kategorie 4: Datenschutz

Wissen über Datenschutz

Datenschutzrichtlinien

Datenschutz und Apps

Kategorie 5: Datenspeicherung und Datenzugriff

Datenzugriff: ungewollt / unbewusst / erlaubt

²²⁶ Vgl. Gläser; Laudel, 2009. S. 201

Sicherheit und Kontrolle der eigenen Daten

Speicherung der eigenen Daten

Kategorie 6: Datenanalyse

Möglichkeiten durch die Speicherung der Daten

Mögliche Folgen für uns

Kategorie 7: Mögliche Folgen von Big Data

Einschätzung / Wissen über Folgen und Vorhersagbarkeit

Eigenes Verhalten / Schutz vor Datenraub und -Speicherung

10. Auswertung

Die Auswertung der Interviews erfolgt mit Hilfe der Kategorien, wobei hier nicht unbedingt ein Vergleich der Antworten angestrebt wird, sondern vielmehr die Tiefenperspektive der Antworten aufgezeigt wird.

10.1. Kategorie 1: Medienkonsum

Bei der Auswertung der ersten Kategorie, Medienkonsum, ist klar ersichtlich, dass das Internet heute bei den jungen Erwachsenen im Alter zwischen 18 und 24 Jahren vorwiegend für die Informationssuche und zur Unterhaltung genutzt wird, dies vor den traditionellen Medien, wie Zeitung und Radio. Außer einer Person nutzen alle Befragten mindestens ein Informationsmedium täglich, das Internet nennt dabei jedeR Befragte. Hier unterscheidet sich das Nutzungsverhalten der Medien aber sehr stark. Während der/die InterviewpartnerIn 5 sich bei speziellen Informationen mit Zeitungen und lokalen Medien, sowie dem Fernsehen informiert²²⁷, sucht der/die InterviewpartnerIn 8 im Internet und auf Internetportalen nach aussagekräftigen Antworten auf spezielle, aktuelle Themen²²⁸. Die Person 10 gibt an, das Internet neben der Informationssuche auch für die Unterhaltung zu nutzen.²²⁹ Allein der/die InterviewpartnerIn 6 versucht Medien aufgrund ihrer zum Teil deprimierenden und negativen Meldungen zu meiden.²³⁰

²²⁷ Vgl. Interview 5: Z 14

²²⁸ Vgl. Interview 8: Z 265-272

²²⁹ Vgl. Interview 10: Z 11-12

²³⁰ Vgl. Interview 6: Z 23-25

10.2. Kategorie 2: Smartphonegebrauch

Bei der Kategorie Smartphonegebrauch zeichnet sich eine starke Nutzung des Smartphones ab. Alle Nutzer verwenden es zum Telefonieren, nutzen das Internet und haben sich Apps heruntergeladen. Bei den weiteren Funktionen wird die Nutzung sehr personalisiert. Außer der Person 11, die für Kurzmitteilungen ausschließlich Facebook und WhatsApp benützt²³¹, schreiben alle Befragten SMS. Besonders Person 11 zeigt Besonderheiten im Smartphonegebrauch auf, weil sie die Nutzung vor allem als Zeitvertreib ansieht. Die restlichen Befragten nutzen ihr Smartphone zur Kommunikation, Unterhaltung und zum Informationsgewinn. Ein besonderes Nutzungsverhalten zeigt auch die Person 5 auf, weil sie im Vergleich zu den anderen Untersuchungspersonen als einzige kein WhatsApp installiert hat und Facebook nur über die Internetseite nutzt²³², während die andern Untersuchungspersonen alle WhatsApp nutzen und sich Facebook auch als App auf ihr Smartphone heruntergeladen haben.

Beim Verhalten hinsichtlich der App-Downloads zeigt sich eine starke Individualisierung, sowohl in der App-Auswahl, wie auch in der Menge der Downloads. Person drei besitzt keinen Computer und benützt ihr Smartphone deshalb für sehr viele Aktivitäten, geht aber beim Herunterladen von Apps sehr bewusst vor. Sie weiß, dass Apps viele Daten von der eignen Person speichern und verwenden können, weshalb sie nur drei Apps heruntergeladen hat. Das Entscheidende für das Herunterladen von Apps ist dabei das persönliche Kosten-Nutzen-Verhältnis²³³.

Während die anderen Untersuchungspersonen im Durchschnitt drei Apps heruntergeladen haben, darunter in erster Linie Facebook und WhatsApp, sowie auch Spiele, Wetter App und Taschenlampen App, hat die Person 9 18 Apps auf ihrem Smartphone installiert, die sie auch alle täglich verwendet. Interessant ist dabei, dass sie sich einen Terminkalender heruntergeladen hat, weil der Terminkalender von Google sich mit ihren anderen Daten synchronisiert und sie das nicht möchte.²³⁴ Auch die Person 10 hat sich im Vergleich mit den anderen Untersuchungspersonen viele Apps heruntergeladen, weiß aber, dass manche Apps schon vorinstalliert auf ihrem Handy waren und besitzt als einzige Untersuchungsperson eine Viren App.²³⁵

²³¹ Vgl. Interview 11: Z 33

²³² Vgl. Interview 5: Z 38-39

²³³ Interview 3: Z 23-25; Z 222-224

²³⁴ Vgl. Interview 9: Z 30-39

²³⁵ Vgl. Interview 10: Z 46-62

10.3. Kategorie 3: Wissen über Big Data

Interessante Ergebnisse zeigen sich bei der Auswertung der Kategorie „Wissen über Big Data“. Außer einer Person, geben alle Untersuchungspersonen an, den Begriff „Big Data“ noch nie gehört zu haben. Person 10 gibt an „Big Data“ schon gehört zu haben, kann sich aber nicht mehr an den Zusammenhang erinnern. Sie stellt sich darunter eine „massive Datensammlung“ vor.²³⁶ Auf die Frage, was unter dem Begriff verstanden wird, fielen die Antworten der anderen UntersuchungsteilnehmerInnen wie folgt aus: „viele Daten, nein keine Ahnung, ich weiß es nicht“,²³⁷ „keine Ahnung“,²³⁸ Person 3 schüttelt verneinend den Kopf,²³⁹ „das hat sicher was mit dem Datenschutz zu tun, und ‚big‘, groß, denk ich mir“,²⁴⁰ „Big Data, große Dateien? Aber ich weiß das jetzt nicht“,²⁴¹ „Datenschutz denke ich mal“,²⁴² „Also ich hoffe es hat jetzt nichts mit einer Date-App zu tun? (...) Nein, ich weiß es nicht“,²⁴³ „irgendein Datennetzwerk, keine Ahnung“,²⁴⁴ „großes Datenvolumen, so was“,²⁴⁵ „Viele Daten, ich weiß nicht. Ansammlung von vielen Daten“.²⁴⁶

10.4. Kategorie 4: Datenschutz

Die Auswertung der Kategorie Datenschutz ergibt im Bereich „Wissen über Datenschutz“, dass zehn Personen der Begriff bekannt ist. Die Person 6 gibt bei der Frage: „Datenschutz ist dir das ein Begriff?“, die Antwort: „Neein, nicht genau.“.²⁴⁷ Die Personen 6, 3 und 2 geben anschließend bei der eigenen Bewertung ihres Wissens über Datenschutz zur Antwort, dass sie sich „gar nicht“,²⁴⁸ „sehr schlecht“²⁴⁹ und sich „eigentlich überhaupt nicht“²⁵⁰ mit Datenschutz auskennen. Der weitere Interviewverlauf zeigt aber auf, dass diese Selbsteinschätzung bei der Person 3 nicht mit ihrem Wissen über Datenschutz übereinstimmt und ihr Verhalten auch nicht im Sinne des Schutzes ihrer Daten korreliert.

²³⁶ Vgl., Interview 10: 70-74

²³⁷ Interview 1: 51

²³⁸ Interview 2: Z 39

²³⁹ Vgl. Interview 3: Z 31

²⁴⁰ Interview 4: Z 49

²⁴¹ Interview 5: Z 64

²⁴² Interview 6: Z 50

²⁴³ Interview 7: Z 61-63

²⁴⁴ Interview 8: Z 61

²⁴⁵ Interview 9: Z 53

²⁴⁶ Interview 11: Z 56

²⁴⁷ Interview 6: Z 54

²⁴⁸ Interview 6: Z 58

²⁴⁹ Interview 2: Z 43

²⁵⁰ Interview 3: Z 35

Die Personen 1, 7, 9 und 10 geben an sich mit dem Datenschutz nicht so gut auszukennen. „Ah, nicht so gut“, ²⁵¹ „Nicht gut“, ²⁵² „Eigentlich nicht gut, ich meine man hört es oft, man hört es auch in den Nachrichten, dass das nicht so geheuer abläuft, oder?“, ²⁵³ „Ich kenne mich mit Datenschutz nicht so gut aus, wenn ich ehrlich bin. Ich vertraue aber auch in diese vielen Unternehmen nicht“. ²⁵⁴ Auch hier zeigt die eigene Einschätzung auf, dass diese nicht mit den Antworten im weiteren Verlauf des Interviews korreliert. Sie weist aber bei den Personen 1 und 9 und besonders bei der Person 10 darauf hin, welche im weiteren Verlauf im Verhältnis sehr aufschlussreiche Antworten geben, dass sie wissen, wie umfangreich der Bereich Datenschutz ist und wie schwierig es ist, sich in diesem Bereich sehr gut auszukennen, wenn man sich nicht sehr intensiv damit befasst.

Die Personen 4, 5, 8 und 11 geben an, sich einigermaßen gut im Bereich Datenschutz auszukennen. „Ja, ein bisschen, jetzt aber nicht, ich bin sicher kein Profi darin“, ²⁵⁵ „Sagen wir so, man hat es auf der Uni ein bisschen gehört, was darf ich verwenden, was darf ich nicht verwenden. Jetzt genau die Gesetze kenn ich nicht“ (I 5, Z 68-69), „Sagen wir recht, ja ein bisschen“ (I 8, Z 65), „Gut, aber ich lege wenig Wert darauf, also mir ist das relativ egal“ (I 11, Z 60).

Eine sehr gute Bewertung hat sich niemand der elf Personen zugetraut. Das mag wohl damit in Verbindung stehen, dass Datenschutz ein sehr breites und tiefläufiges Themengebiet ist, welches – angelehnt an die Gesetze – mit seinen vielen Facetten schwer zu verstehen ist.

Unter dem Begriff Datenschutz haben die InterviewpartnerInnen unterschiedliche Auffassungen. Vier Personen, die InterviewpartnerInnen 1, 2, 3 und 9, verstehen darunter, dass ihre Daten geschützt werden, besonders im Hinblick auf eine Veröffentlichung. Die Personen 1 und 2 verstehen darunter zudem, dass sie nicht für jedermann zugänglich sind und somit auch nicht von anderen beispielsweise im Internet gesucht werden können. Die Person 9 verbindet den Datenschutz auch mit einer nicht erlaubten Weitergabe ihrer Daten. Interessant ist, dass die Person 3 Facebook als Beispiel nimmt und erklärt, „dass die Fotos auch wirklich dort bleiben, auch wenn man sie löscht, gehören sie dann

²⁵¹ Interview 1: Z 55

²⁵² Interview 7: Z 67

²⁵³ Interview 9: Z 57-58

²⁵⁴ Interview 10: Z 78-79

²⁵⁵ Interview 4: Z 55

Facebook“.²⁵⁶ Sie betont, dass sie sich mit dem Thema Datenschutz nie sehr stark beschäftigt hat, weil ihr noch nie etwas passiert sei, im Sinne von Viren oder Hackern. Auf die genaue Nachfrage der Autorin im Hinblick auf Viren oder Hackerangriffe äußert sie jedoch Zweifel. Sie habe zwar nichts bemerkt, aber sie weiß, dass es dennoch so hätte sein können.²⁵⁷

Der/die InterviewpartnerIn 4 weiß, dass überall wo man Daten eingibt, die Firma, die die Daten erhält, in der Datenschutzerklärung mitteilt, dass die Daten geschützt werden.²⁵⁸ Ebenso verstehen die Personen 7 und 11 unter dem Datenschutz den Schutz ihrer Daten.²⁵⁹ Person 6 fügt dem noch hinzu, dass ihre Daten nicht weitergegeben werden an Dritte.²⁶⁰

Eine sehr ausführliche und treffende Erklärung zum Thema Datenschutz geben die InterviewpartnerInnen 8 und 10. Die Person 8 äußert sich dazu: „wenn ich irgendwo meine Daten eingeben muss, ist immer ein Datenschutz dabei, den ich dann bestätigen muss oder unterschreiben muss, dass meine Daten nicht weitergegeben werden. Also sie bestätigen mir gegebenenfalls in diesem Fall, dass diese Daten nur für bestimmte Zwecke benutzt werden und nicht veröffentlicht werden oder missbraucht werden“,²⁶¹ als Zwecke führt sie Studien an, bei denen sie glaubt, dass es sich um Nachfragen oder um die Marktentwicklung handelt.²⁶²

Der/die InterviewpartnerIn 10 erklärt, dass es in Situationen, in denen man eigene Daten angeben muss, ein Abkommen zwischen ihm/ihr und dem Vertragspartner gibt, worin festgelegt wird, für was die eigenen Daten verwendet werden dürfen und dass sie nicht ohne Erlaubnis an Dritte weitergegeben werden.²⁶³

Die Person 5 erklärt, dass es innerhalb des Datenschutzes Rechte und Pflichten gibt, welche man beachten muss, wenn man Daten anderer Personen verwendet. Sie geht hier auch genau auf das Plagiat und das Filmstreaming als Beispiel unerlaubter Datenverwendung ein.²⁶⁴

Im Hinblick auf den Datenschutz und dessen Richtlinien und Bestimmungen, ist allen TeilnehmerInnen der Begriff Datenschutzrichtlinie oder –Bestimmung bekannt, außer der

²⁵⁶ Interview 3: Z 42-43

²⁵⁷ Vgl. Interview 3: Z 43-49

²⁵⁸ Vgl. Interview 4: Z 57-62

²⁵⁹ Vgl. Interview 7: Z 69; Interview 11: Z 62

²⁶⁰ Vgl. Interview 6: Z 60-61

²⁶¹ Interview 8: Z 68-72

²⁶² Vgl. Interview 8: Z 74-76

²⁶³ Vgl. Interview 10: Z 82-88

²⁶⁴ Vgl. Interview 5: Z 72-92

Person 2, die angibt, diese Begriffe noch nie gehört zu haben. Interessant ist dabei jedoch, dass die Person zwar angibt nicht zu wissen, was in einer Datenschutzrichtlinie drinnen steht, sie aber meint, schon mal eine unterschrieben, bzw. akzeptiert zu haben. Sie nennt hier als Beispiel Facebook: „Wenn du dich heute bei Facebook und so anmeldest und wo du anklicken musst, was keiner durchliest, damit es immer weiter geht“.²⁶⁵ Alle anderen Personen sind sich sicher, dass sie eine Datenschutzerklärung bereits unterzeichnet haben, Person 1 nennt als Beispiel die Banken, und kommt im Laufe des Interviews drauf, dass auch Apps Datenschutzerklärungen haben.²⁶⁶ Person 8 nennt einen wichtigen Aspekt, nämlich, dass man eine Datenrichtlinie eigentlich häufig unterschreibt, auch wenn es einem oft nicht bewusst ist²⁶⁷. Auch der Person 10 ist es bewusst, dass man „permanent“ Datenschutzerklärungen unterzeichnet.²⁶⁸ Auffallend ist, dass nicht nur die TeilnehmerInnen selbst meistens die Bestimmungen nicht lesen, neun TeilnehmerInnen geben an die Bedingungen nicht zu lesen, sondern sie sind auch der Überzeugung, dass andere Personen dies ebenfalls nicht machen.²⁶⁹ Person 8 nennt als Grund, dass diese zu lang und kompliziert verfasst seien²⁷⁰, ist sich aber bewusst, dass man in diesem Bereich zu leichtsinnig vorgeht.²⁷¹ Person 11 denkt hingegen, dass der Datenschutz viele Personen nicht interessiert und deshalb auch keine Beachtung erhält.²⁷² Person 4 gibt an, zwar schon mal eine Richtlinie durchgelesen zu haben, aber noch keine von den Apps.²⁷³ Die Person 5 hingegen liest sich die Richtlinien nicht durch, außer jene, die sie (persönlich, nicht digital) unterschreibt, weil diese meistens kurz gehalten sind. Sie schaut sich dafür aber bei den Apps genau an, auf welche Bereiche sie Zugriff verlangen.²⁷⁴

Auf die Frage, ob ihre Apps eigene Datenschutzerklärungen haben, antworten sieben Personen mit ja, wobei die Personen 2 und 3 sich unsicher sind. Person 7 antwortet mit nein und Person 6 denkt, dass die „normalen“ Apps, wie Facebook und WhatsApp, dies schon besitzen, aber „außergewöhnliche“ Apps nicht.²⁷⁵

Auf die Frage, wo man sich über die Datenschutzerklärungen der einzelnen Dienste informieren kann, vermuten, außer der Person 5, alle Personen bei den Apps selbst.

²⁶⁵ Interview 2: Z 57-58

²⁶⁶ Vgl. Interview 1: Z 101-103

²⁶⁷ Vgl. Interview 8: Z 83

²⁶⁸ Vgl. Interview 10: Z 99

²⁶⁹ Vgl. Interview 1: Z 101; Interview 3: Z 80; Interview 11: Z 74-74

²⁷⁰ Vgl. Interview 8: Z 97; vgl. auch: Interview 4: Z 91-92; Interview 6: Z 86

²⁷¹ Vgl. Interview 8: Z 95

²⁷² Vgl. Interview 11: Z 74-75

²⁷³ Vgl. Interview 4: Z 72, 94

²⁷⁴ Vgl. Interview 5: Z 106, 116-117, 122

²⁷⁵ Vgl. Interview 6: Z 80-84

Person 5 gibt hier das Internet, sowie die Verbraucherzentrale an. Die Verbraucherzentrale nennt auch Person 10.²⁷⁶ Das Internet als Option nennen zusätzlich Person 1, 6, und 11.²⁷⁷

Die Untersuchung möchte vor allem das Wissen der einzelnen Personen untersuchen, weshalb bei der Fragen hinsichtlich des Inhaltes einer Datenschutzrichtlinie die Antworten der TeilnehmerInnen einzeln ausgewertet werden.

Die Person 1 gibt im Interview an, die Datenschutzrichtlinien von Apps nicht zu lesen,²⁷⁸ womit sie natürlich auch nicht mit Sicherheit antworten kann, was in einer Datenschutzrichtlinie steht, bzw. welche Datenschutzbestimmungen ihre Apps haben.²⁷⁹ Besonders interessant ist deshalb, dass die Person vermutet, dass in der Datenschutzerklärung aufgelistet wird, was und wie viel über ihr online und offline Verhalten gespeichert wird. Sie nennt explizit Internetsuchverläufe, Uhrzeit, Kontakte, Standorte.²⁸⁰ Bei der Frage auf welche Daten eine App zugreifen kann beim Smartphone des/der Befragten, vermutet er/sie auf den Standort, die Adressanten von SMS und Telefonaten und den Zeitpunkt des Kontaktes. Ob es auch möglich ist, dass Fremde die Nachricht lesen, weiß der/die Befragte nicht, denkt aber, dass es irgendwie sicher möglich sei. Er/sie zweifelt deshalb, weil er/sie nicht weiß, aus welchem Grund die persönlichen Nachrichten für andere interessant sein können.²⁸¹ Die Person weiß, dass ihre Daten dazu genutzt werden, um ein Profil von ihr zu erstellen, womit die ihr zugesandte Werbung sie bestmöglich anspricht und damit ein Kauf begünstigt wird.²⁸²

Person 2 gibt an, den Begriff Datenschutzrichtlinie oder –Bestimmung nicht zu kennen und erklärt, dass sie nicht weiß, was in einer solchen drinnen steht bzw. sich auch nie eine Bestimmung durchgelesen hat.²⁸³ Sie vermutet, dass mit den Datenschutzrichtlinien ihrer Apps die privaten Daten auf ihrem Handy vor dem Zugriff von Apps und anderen Personen geschützt sind. „Wenn du Fotos machst, dass Facebook dann nicht das von deinem Handy herunternehmen kann oder ansehen kann. Solche Sachen denke ich mir,

²⁷⁶ Vgl. Interview 10: Z 111-112

²⁷⁷ Vgl. Interview 1: Z 96-99, Interview 6: Z 90-95; Interview 11: Z 102-104

²⁷⁸ Vgl. Interview 1: Z 85

²⁷⁹ Vgl. Interview 1: Z 71, 87

²⁸⁰ Vgl. Interview 1: Z 88-93

²⁸¹ Interview 1: Z 104-111

²⁸² Interview 1: Z 114-117

²⁸³ Vgl. Interview 2: Z 51-53, 55, 64

hauptsächlich“.²⁸⁴ Sie weiß, dass man sich bei den Apps über die geltenden Richtlinien informieren kann und diese auch immer vor der Installation akzeptieren muss.²⁸⁵ Auf die Frage auf welche Daten ihre Apps auf ihrem Handy zugreifen können, antwortet die Person 2: „Ich hoffe auf keine. Aber wenn, dann denke ich zum Beispiel Facebook vor allem, was man liked und so. Denk ich mir. Oder Kommentare oder wenn du was erwähnst oder so.“²⁸⁶ Apps können laut ihr „auf Telefonnummern und so denke ich weniger, Fotos und solche Sachen“ eher zugreifen.²⁸⁷

Person 3 meint, dass in einer Datenschutzbestimmung drinnen steht, „dass sie die Daten weitergeben können, oder dass sie über diese verfügen können, dass das ihnen dann gehört wahrscheinlich“.²⁸⁸ Die Person 3 äußert sich zudem: „Mein Problem ist, dass ich nicht verstehe, warum, also was sie dann mit diesen Daten tun, weil so interessant bin ich jetzt nicht.“²⁸⁹ Sie spricht damit einen entscheidenden Faktor an, nämlich das Verständnis für die wirtschaftliche Motivation, welche Big Data antreibt. Wie Constanze Kurz und Frank Rieger beschreiben, ist es ausschlaggebend die finanziellen Mechanismen zu durchblicken, um die daraus resultierenden Motivationen der Menschen und Institutionen zu erkennen.²⁹⁰ Auf die Frage, welche Datenschutzrichtlinien ihre Apps haben, antwortet die Person 3, sie glaubt, dass es hierbei vor allem um die Privatsphäre geht und auch um Daten, wie zum Beispiel Fotos, dass diese im Besitz der Anbieter sind, sobald man sie ein Mal zur Verfügung gestellt hat. „Und um die Fotos, das ist das, was ich mir jetzt schon bewusst bin, dass wenn ich etwas reinstelle, dass auch, wenn ich es lösche, dass es dann immer wieder verwendet werden kann.“²⁹¹ Sehr interessant ist, dass die Person auf die Frage nach dem Datenzugriff ihrer Apps auf die aktuellen Geschehnisse der vergangenen Monate Bezug nimmt. „Ich glaube, also das was ich jetzt auch so gehört habe, das war jetzt ja Thema. Glaub ich grundsätzlich auf alles. (...) Handynummer, Nachrichten, man hat ja gehört, dass sie jetzt wirklich auch im Stande sind, die Nachrichten, die E-Mails, dass sie das wirklich mehr oder weniger lesen.“²⁹² Diese Informationen entnahm die

²⁸⁴ Interview 2: Z 71-72

²⁸⁵ Vgl. Interview 2: Z 76-81

²⁸⁶ Interview 2: Z 84-85

²⁸⁷ Interview 2: Z 122-123

²⁸⁸ Interview 3: Z 55-56

²⁸⁹ Interview 3: Z 57-58

²⁹⁰ Vgl. Kurz; Rieger, 2011. S. 9

²⁹¹ Interview 3: Z 66-69

²⁹² Interview 3: Z 84-85; 87-88

Person den Nachrichten im Fernsehen über Veröffentlichungen von Promis.²⁹³ Der/die Befragte berichtet zudem, dass der Zugriff auf das Smartphone durch die heruntergeladenen Apps ermöglicht wird. Er/sie beschreibt den Zugriff als Zugriff auf eine App, wobei ihm/ihr bewusst ist, dass es auch einen Zugriff auf das Smartphone gibt, weil ansonsten private Nachrichten, die nicht auf der App gespeichert sind, vom Zugriff ausgeschlossen wären, was aber laut seinem/ihrem Wissen nicht der Fall war.²⁹⁴ Es ist der Person 3 bewusst, dass alle Daten auf ihrem Handy für andere grundsätzlich einsehbar sind.²⁹⁵

Person 4 weiß was eine Datenschutzrichtlinie ist.²⁹⁶ Sie liest sich diese von den Apps zwar nicht durch, weiß aber von einer anderen Datenschutzerklärung, die sie sich durchgelesen hat, dass darin die Verwendung ihrer Daten durch die jeweilige Firma geregelt ist und für eine Verwendung der Daten die Zustimmung erteilt werden muss.²⁹⁷ Interessant ist dabei, dass sie zwar weiß, dass die App in der Datenschutzrichtlinie festlegen kann welche und wie viele Daten sie verwenden kann,²⁹⁸ sie aber der Meinung ist, dass ihre Apps nicht auf Daten auf ihrem Handy zugreifen können.²⁹⁹ Der/die InterviewpartnerIn gibt an, dass ihre Apps keinen Zugriff auf sein/ihr Smartphone und damit auf persönliche Daten, wie Fotos, Kontaktdaten im Adressbuch, Kalendernotizen hätten, und dass er/sie kontrolliert, ob jemand Zugriff auf sein/ihr Smartphone und seine/ihre Daten verlangt, spricht dabei aber vorwiegend von der Anfrage zu einem Verbindungsaufbau zum Internet.³⁰⁰ Beim genaueren Nachfragen, ob sie es für möglich hält, dass sich die App auch ohne um Erlaubnis zu fragen verbinden könnte, verneint sie dies, hält es anschließend aber dann doch für möglich, dass man bereits in der Zustimmung der Datenschutzrichtlinien den Apps diese Erlaubnis erteilt haben kann.³⁰¹ Im weiteren Verlauf des Interviews ist sie jedoch wieder anderer Meinung: „Ich unterschreibe ja, dass sie meine Daten verwenden dürfen, aber, dass sie ohne Erlaubnis Daten von meinem Handy verwenden können, das steht sicher in einer

²⁹³ Vgl. Interview 3: 90-91

²⁹⁴ Vgl. Interview 3: Z 94-95; 97-100

²⁹⁵ Vgl. Interview 3: Z 101-102

²⁹⁶ Interview 4: Z 63-64

²⁹⁷ Interview 4: Z 72-74

²⁹⁸ Interview 4: Z 78-79

²⁹⁹ Vgl. Interview 4: Z 99

³⁰⁰ Vgl. Interview 4: Z 95-103

³⁰¹ Vgl. Interview 133-137

Datenschutzrichtlinie drinnen, dass sie das nicht dürfen. (...), aber sie machen das oft trotzdem. Das merkst du ja nicht mal, wenn sie sie nehmen oder nicht.“³⁰²

Person 5 hat sich eine Datenschutzrichtlinie noch nie durchgelesen, weshalb sie auch nicht weiß, welche Datenschutzrichtlinien ihre Apps haben. Generell vermutet sie, dass in einer Richtlinie klar formuliert ist, was erlaubt ist, bzw. nicht erlaubt ist und dies vor allem die Persönlichkeit einer Person schützen soll.³⁰³ Sie kontrolliert bei einer Installation einer neuen App auf welche Bereiche diese zugreifen möchte. Die Person weiß deshalb, dass die meisten Apps den Zugriff auf Fotodateien verlangen. Zudem erinnert sie sich, dass manche Apps auch den Zugriff auf Kreditkarteninformationen wollten, welcher sie sehr erschreckt hat. Sie berichtet weiter, dass sie auch Apps bereits wieder gelöscht hat, weil sie sie nicht benutzte.³⁰⁴

Der Begriff Datenschutzrichtlinie ist der Person 6 zwar bekannt, aber sie ist sich nicht sicher, ob alle ihre Apps Datenschutzrichtlinien haben und weiß infolge auch nicht welche Datenschutzrichtlinien ihre Apps haben.³⁰⁵ Sie kann sich generell unter einer Datenschutzrichtlinie vorstellen, dass darin festgehalten wird, dass ihre Daten nicht an Dritte weitergegeben werden.³⁰⁶ Interessant ist die Antwort auf die Frage auf welche Daten die App Zugriff hat, dass die Person 6 den Zugriff auf Telefonnummern angibt, beim Zugriff auf das Adressbuch ist sie unsicher. Vor allem aber weiß sie nicht, dass die App Zugriff auf ihre Fotos hat, sie meint nur auf die Fotos, die sie hochladet, nicht aber jene, die sie auf ihrem Handy hat und nicht hochgeladen hat, obwohl sie erklärt, dass man den Zugriff erlauben muss, wobei sie dabei nicht den Zugriff auf ihren Fotoordner meint, sondern auf Fotos, die sie hochladet.³⁰⁷

Der/Die Befragte 7 kennt sich mit dem Thema Datenschutz zwar nicht gut aus, weiß aber aufgrund von eigenen Erfahrungen mit Facebook-Profilbildern und der lokalen Zeitung, dass ihre Daten, wie Fotos, für Zwecke verwendet werden dürfen, denen sie in der Datenschutzrichtlinie zustimmt.³⁰⁸ Auf die Frage, ob Apps Zugriff auf ihre persönlichen Daten am Smartphone haben, reagiert die Person erschrocken: „Meine Apps, meine

³⁰² Interview 4: Z 227-229; 233-234

³⁰³ Vgl. Interview 5: Z 98-104

³⁰⁴ Vgl. Interview 5: Z 130-134

³⁰⁵ Vgl. Interview 6: Z 79-84, 87-89

³⁰⁶ Vgl. Interview 6: Z 66

³⁰⁷ Vgl. Interview 6: Z 108, 112-114

³⁰⁸ Vgl. Interview 7: Z 100-107

Daten [sehr erschrocken]. Das hoff ich wohl nicht, dass meine Apps auf meine Daten zugreifen können.“³⁰⁹ Sie weiß nicht, dass Facebook Zugriff zu ihren Fotos auf ihrem Handy haben kann, und WhatsApp auf die Nummern in ihrem Adressbuch.³¹⁰ Sie hat jedoch beobachtet, dass nach dem Versenden einer E-Mail die entsprechende E-Mailadresse automatisch beim dazugehörigen Kontakt in ihrem Adressbuch aufscheint. Sie glaubt daher, dass Gmail, bzw. Google Zugriff auf ihr Smartphone hat und Daten synchronisiert werden. Den Zugriff auf ihre Fotos muss sie Gmail, bzw. Google aber erst erlauben mit der Zustimmung, wobei sie hier die Synchronisation mit dem Smartphone-Hersteller meint, weil sie im weiteren erklärt, dass somit die Fotos auch bei Verlust des Smartphone gesichert sind. Sie weiß nicht genau, wo und wie das funktioniert.³¹¹

Die Person 8 zeigt ein sehr gutes Verständnis im Bereich Datenschutz und weiß, dass die Datenschutzrichtlinien Aufschluss darüber geben, für welchen Zweck und von wem verwendet werden.³¹² Als einziger TeilnehmerIn erwähnt sie im weiteren Verlauf des Interviews, dass sie sich die Zeit nimmt, um eventuelle Änderungen bei den Datenschutzrichtlinien von Diensten auch genau durchzulesen. Sie spricht hier konkret Facebook an: „wenn es neue Einstellungen gibt. Dann schau ich auch ob sich da etwas in meiner Sicherung verändert hat oder hat sich das nun alles veröffentlicht, so zu sagen.“³¹³ Zwar wissen 10 TeilnehmerInnen, dass sie sich bei den Datenschutzrichtlinien über die Verwendung ihrer Daten informieren können, Person 8 ist aber die einzige, die in dieser Untersuchungsgruppe angibt, dies auch wirklich zu tun. Denn zwischen bloßem Wissen und dem entsprechenden Verhalten liegt ein Unterschied, der entscheidend für unsere Sicherheit hinsichtlich der Verwendung unserer Daten ist. Auch spricht die Person 8 in diesem Zusammenhang von Medien. „Man bekommt ja viel mit in den Medien.“³¹⁴ Der/die Befragte ist der Meinung, dass der Datenzugriff einer jeden App unterschiedlich gestaltet sein kann. Sie weiß, dass sie auf jeden Fall auf jene Daten zugreifen kann, die man selbst an die Apps gibt. Den Zugriff auf Fotos und dergl. kann man bei manchen Apps ebenso freiwillig erlauben oder verweigern. Im Hinblick auf die Nachrichtenportale

³⁰⁹ Interview 7: Z 126-127

³¹⁰ Vgl. Interview 7: Z 128-134

³¹¹ Vgl. Interview 7: Z 135-153

³¹² Vgl. Interview 8: Z 81, 99-100

³¹³ Vgl. Interview 8: Z 258-260

³¹⁴ Interview 8: Z 256

ist sich die Person bewusst, dass diese auf ihre gesamten Nachrichten, wie auch das Adressbuch zugreifen können.³¹⁵

Die Person 9 versteht unter dem Datenschutz, dass bei einer Registration eines gewissen Dienstes oder Vereins ihre persönlichen Daten nur auf dieser Seite bleiben und nicht in die Öffentlichkeit gelangen, sowie auch nicht an Dritte weitergegeben werden dürfen. Sie ist sich zwar bewusst, dass ihre Daten gespeichert werden, denkt aber nicht, dass es erlaubt ist, ihre Daten für Analysen und Programme zu verwenden.³¹⁶ Beim Zugriff auf ihre Daten denkt die Person im ersten Moment nur an jene Daten, die sie bei der Registration eingibt³¹⁷, kann sich beim Beispiel Facebook aber schon vorstellen, dass Facebook auch auf am Smartphone gespeicherte Fotos zugreifen kann. Sie erklärt sich das somit: „Wenn du ein Foto auswählst für Facebook, dann siehst du da ja auch schon alle, obwohl du sie nicht raufgeladen hast.“³¹⁸

Person 10 zeigt ein sehr gutes Verständnis im Bereich des Datenschutzes und den wirtschaftlichen Faktoren. Sie weiß, dass ihre Apps persönliche Daten an Dritte weitergeben. Bewusst ist ihr das unter anderem auch durch personalisierte Werbeanzeigen nach einer Suchanfrage auf Google.³¹⁹ Auf die Frage nach dem Datenzugriff von Apps verweist die Person darauf, dass Google sie darauf hinweist, welche Daten bezogen werden. Generell nennt sie Mitteilungen, den Suchverlauf des Internets, Kreditkarteninformationen und Medien, wie Videos, Musik und Fotos, die auf dem Smartphone gespeichert sind.³²⁰

Die Person 11 gibt an, dass sie sich gut auskennt im Bereich des Datenschutzes, aber kein spezielles Interesse an der Information darüber hat.³²¹ Sie weiß nicht genau, was in einer Datenschutzrichtlinie drinnen steht, denkt aber, dass ihre Daten nicht weitergegeben werden und geschützt werden. Auch den Zugriff ihrer Daten durch interne Mitarbeiter, sowie die Benützung der Daten oder deren Verkauf und dergleichen schließt sie aus.³²² Wenn sie an ihre Apps denkt, ist sie der Meinung, dass diese relativ schwache

³¹⁵ Vgl. Interview 8: Z 105-116

³¹⁶ Vgl. Interview 9: Z 74-75, 84-87

³¹⁷ Interview 9: Z 113

³¹⁸ Interview 9: Z 124-125

³¹⁹ Vgl. Interview 10: Z 103-114

³²⁰ Vgl. Interview 10: Z 115-126

³²¹ Vgl. Interview 11: Z 60

³²² Vgl. Interview 11: Z 69-71

Datenschutzrichtlinien haben und die Sicherung unzureichend ist. Sie verweist an dieser Stelle auf die Berichte in den Medien, aus denen sie die Informationen über Probleme bei Facebook entnimmt.³²³ Besonders bei kleineren Apps denkt sie, dass die Sicherung nicht gut ist und viele Daten unbewusst weitergegeben oder gestohlen werden.³²⁴ Ihr ist durch die Meldungen von Apps, wie zum Beispiel Instagram, bewusst, dass diese Apps auf ihre Fotos zugreifen können, aber auch auf ihre Kontakte, weil sie sonst nicht funktionieren könnten.³²⁵

10.5. Kategorie 5: Datenspeicherung und Datenzugriff

Die Auswertung des ersten Szenarios ergibt ein sehr klares Bild über den aktuellen Wissenstand der Befragten. Außer der Person 4 sind alle UntersuchungsteilnehmerInnen von der Möglichkeit überzeugt, dass fremde Personen sich Daten des eigenen Smartphone ansehen können. Die Personen 2, 5, 6, 7, 8, 10 und 11 denken dabei zuerst an illegale Möglichkeiten, sind aber bei genauer Nachfrage auch davon überzeugt, dass es auch auf legalem Weg geht. Obwohl die Person 3 denkt, dass es eine legale Möglichkeit gibt, äußert sie nicht, an welche sie dabei denkt. Die Personen 1, 2, 5, 6, 10 und 11 erklären anfangs die Möglichkeit des Zugriffes über das Internet, wobei sie hier unerlaubte Handlungen ansprechen. Bei genauerer Nachfrage bekunden sie aber gemeinsam mit den Personen 7, 8 und 9, dass es durchaus möglich sei, die Erlaubnis durch das Zustimmung der Datenschutzrichtlinien zu erteilen. Ob diese Erlaubniserteilung den SmartphonebesitzerInnen stets bewusst ist, daran zweifeln viele, eben weil die Datenschutzrichtlinien nur minimale Beachtung finden. Person 10 formuliert diesen Sachverhalte sehr treffend: „Dass er ihnen das erlaubt, ihm das aber nicht bewusst ist, darin bin ich voll überzeugt, dass das der Fall ist.“³²⁶

Auf die anschließende Frage wie gut die eigenen Fotos auf dem Smartphone geschützt sind, antwortet die Person 8 als einzige gut, in dem Umfang in dem sie sie schützen kann.³²⁷ Die Personen 2, 4, 5 und 6 hoffen lediglich, dass sie gut geschützt sind. Als Begründung geben sie an, dass sie nicht viele Apps runterladen³²⁸ oder nur Fotos von sich

³²³ Vgl. Interview 11: Z 89-92

³²⁴ Vgl. Interview 11: Z 98-99

³²⁵ Vgl. Interview 11: Z 105-121

³²⁶ Interview 10: Z 150-151

³²⁷ Vgl. Interview 8: Z 138-146

³²⁸ Vgl. Interview 2: Z 105-106

machen lassen, die jeder Fremde unbedenklich sehen darf³²⁹. Die Person 6 ist sich hingegen unsicher, da sie nicht weiß, welchen Bedingungen sie in den Datenschutzrichtlinie zugestimmt hat.³³⁰ Die Person 1 weiß, dass ihre Fotos überhaupt nicht geschützt sind, die Personen 3,7,9,10 und 11 denken hingegen nicht gut. Interessant ist, dass Person 9 an dieser Stelle auf die Apps verweist: „Also auf dem Handy selbst, da habe ich auch einen Sicherheitscode oder ein Muster, dass man überhaupt nichts sieht, aber durch die Apps eigentlich haben dann doch wieder viele Zugriff, eigentlich schon.“³³¹ Dass sie selbst die Sicherheit ihrer Daten beeinflussen können, wissen dabei alle Untersuchungspersonen außer der Person 11. Sie gibt an, keinen Einfluss auf die Datenspeicherung von Apps zu haben.³³² Interessant ist hier jedoch, dass sechs Personen anschließend sagen, dass sie jedoch nicht kontrollieren können auf welche Daten Apps zugreifen.

Wenn, gefolgt an das erste Szenario die Frage gestellt wird, wer außer der jeweiligen Person noch alles Zugriff auf ihr Smartphone hat, dann zeichnet sich ab, dass das Hintergrundwissen der Personen hinsichtlich ihres eigenen Verhaltens am Smartphone doch nicht so ausgeprägt ist.

So geben die Personen 1 und 2 an, dass niemand Zugriff hätte, zumindest hoffen sie dies. Person 1 erwähnt, niemand wissentlich den Zugriff erlaubt zu haben. Die Person 2 schließt dem an, dass es große Firmen geben kann, die den Zugriff vielleicht erhalten haben könnten. Nicht genau darüber Bescheid wissen die Personen 3 und 6, wobei die Personen 3, 4 und 6 davon ausgehen, dass es Apps sind, die auf ihr Handy zugreifen können. Die Person 8 spricht sogar von fast jeder App.³³³

Auf die zentrale Frage für das Verständnis der Datenspeicherung und –Auswertung, wieso sich Unternehmen die Zugriffserlaubnis auf persönliche Daten am Smartphone einholen, weiß die Person 3 keine genaue Antwort: „Ja man hört ja immer wieder mal von Hackern und so. Aber jetzt für was genau und warum, das weiß ich nicht. Ich glaub die App selbst hat keinen Nutzen davon, wenn dann ist es jemand im Hintergrund, der sich vielleicht Daten herunterlädt oder so.“³³⁴ Die Person 10 hingegen erläutert sehr detailliert, wieso Apps absichtlich Funktionen ergänzen, um an noch mehr Daten zu kommen: „Ja

³²⁹ Vgl. Interview 5: Z 195-200

³³⁰ Vgl. Interview 6: Z 154-157

³³¹ Interview 9: Z 142-146

³³² Vgl. Interview 11: Z 141-148

³³³ Vgl. Interview 8: Z 158

³³⁴ Interview 3: Z 176-178

wegen der Wirtschaft in erster Linie. Ich meine solche Unternehmen wie Facebook oder so, diese müssen sich irgendwie finanzieren, eigentlich das ist ja gratis das ganze Ding, sie brauchen aber doch für diese ganze Serverkapazität, brauchen sie Geld. Dein Account und das. Das machen sie einmal durch aktive Werbeschaltung und durch die Information, durch deine Verbrauch-Information, an Unternehmen und dann bekommst du ja diese maßgeschneiderte Werbung zu dir zugeliefert, dass sie dich mehr oder weniger genau mit dem bombardieren, für was du dich informierst“.³³⁵

Auch die Personen 1, 2, 6 und 7 sind davon überzeugt, dass der Datenzugriff der Finanzierung der App durch Werbung dient. Sehr interessant ist dabei die Antwort der Person 6: „Bo, weil sie das sammeln und dass sie einfach wissen, wer zu wem gehört und irgendwie keine Ahnung, dass das irgendwie alles vernetzt ist. (...) Bo, ich glaube ich hab mal gehört, dass man diese Daten auch verkaufen kann, dass man da auch so Handel machen kann. Ich weiß nicht, dann bekommst du auch Werbungen zugeschickt, von diesen Sachen.“³³⁶ Die Personen 1 und 7 sprechen zusammen mit den Personen 4, 5, 8, 9, und 11 auch die Funktionsausführung der App an. Die Person 11 nennt im weiteren Gesprächsverlauf auch die Möglichkeit des Datenverkaufs oder der Werbung. Sie erklärt: „Daten sind immer beliebt. Also ich denke unabhängig, ob das alles brauchbare Daten sind, je mehr du hast, hast du halt viele. (...) Je mehr Daten du hast, umso mehr Personen erreichst du.“³³⁷ Auffallend ist, dass die Person 9 die Datenspeicherung in Verbindung zu den Geheimdiensten und einer Kontrolle bringt.³³⁸ Sehr ausführlich beschreibt dieses Zusammenspiel auch die Person 10, die als weiteres Ziel der Datensammlung den Staat und die Geheimdienste anspricht und dabei auf die aktuelle Berichterstattung über Google eingetht: „Naja, für den Staat, wie man jetzt bei den NSA herausgefunden hat, ist Spionage auch interessant. Wie man da gehört hat, haben sie da auch auf die Google-Server zugegriffen.“³³⁹ Der/die Befragte zeigt ein sehr gutes Verständnis der wirtschaftlichen und staatlichen Faktoren auf: „Ja, das eine ist Wirtschaftsspionage, nicht direkt aber halt so. Und das andere ist die aktive Kontrolle von der Masse. Wenn du die Masse kontrollieren kannst, beziehungsweise ihre Gedanken nachvollziehen, hast du als Staat mehr Macht und mehr Kontrolle über dein eigenes Volk.“³⁴⁰

³³⁵ Interview 10: Z 174-180

³³⁶ Interview 6: Z185-186; 189-191

³³⁷ Interview 11: Z 183-184; 192-193

³³⁸ Vgl. Interview 9: Z 184-192

³³⁹ Interview 10: Z 192-193

³⁴⁰ Interview 10: Z 194-198

10.6. Kategorie 6: Datenanalyse

Sehr interessante Ergebnisse liefert die Auswertung der Kategorie Datenanalyse. Auf die Frage was Unternehmen machen können, wenn sie nicht nur unsere Daten, sondern auch Daten von unzählig vielen anderen Personen besitzen, ist sich der Großteil der Befragten einig: Werbung nennen hier die Personen 2, 4, 5, 6, 7 und 11. Die Personen 1, 3 und 7 sind sich unsicher. Die Personen 1 und 8 denken an Erpressung³⁴¹, 3 und 8 nennen Ausnutzung der Daten³⁴² und die Personen 3 und 9 die eigene Überprüfung.³⁴³ Person 5 nennt Kontrolle, Person 11 Macht als Resultat. Obwohl die Person 8 beim restlichen Interview ein sehr gutes Verständnis für Datenschutz und den Möglichkeiten und Risiken bewiesen hat, ist sie „überfragt“³⁴⁴, wenn es darum geht die Verarbeitungsschritte der Datenspeicherung zu erklären.

Sehr ausführlich und detailliert erklärt die Person 10 die Möglichkeiten des Unternehmens: „Ja zuerst mal in Datenbanken einspeichern, Datenbanken vergleichen und durch irgendwelche komplizierte Programme durchlaufen lassen, die Programme dann noch filtern, was du so suchst. Und dir dann automatisch wieder – ihnen Information mehr oder weniger was diese Person, natürlich macht das alles ein Computer, weil für einen Menschen wäre das zu viel. (...) Ja, sie werden analysiert und verarbeitet, ich meine natürlich wird von Person XY, werden jetzt nicht Mitarbeiter, Bilder zu sehen bekommen. Sie können es, wenn sie wollen, aber ich glaube nicht, dass mein Bild irgendjemand, keine Ahnung, der in Kalifornien in einer Zentrale arbeitet, alle meine Bilder sieht. Natürlich können sie es, wenn sie wollen, aber ich sage, das wird automatisch verarbeitet.“³⁴⁵

Als Folgen, die sich für uns aus einer derartigen Datenspeicherung ergeben können, nennen die Personen 2, 3 und 9 eine eingeschränkte Privatsphäre. Die Person 3 befürchtet, dass es sich soweit entwickeln kann, dass wir überhaupt keine Privatsphäre mehr haben, „dass wir immer überwacht werden, also immer kontrolliert werden können wo wir sind und was wir machen. (...) dass man halt überhaupt nichts mehr schützen kann, dass man eigentlich ein offenes Buch ist.“³⁴⁶ Von einer Überwachung sprechen neben der Person 3 auch die Personen 5 und 9, wobei sie hier auch explizit ansprechen,

³⁴¹ Interview 1: Z 178; Interview 8: Z 203-204

³⁴² Interview 3: Z 189; Interview 8: Z 203-204

³⁴³ Interview 3: Z 189; Interview 9: Z 197

³⁴⁴ Interview 8: Z 217

³⁴⁵ Interview 10: Z 201-211

³⁴⁶ Interview 3: Z 192-193; 195-196

dass es vor allem unangenehm ist, zu wissen, dass man bei allem überwacht wird.³⁴⁷ Die Person 3 sieht es hier auch als Einschnitt in die Privatsphäre, weil infolge der Datenspeicherung auch das Verhalten beeinflusst wird - man verhält sich anders, wenn man weiß, man wird beobachtet.³⁴⁸ Vor allem Werbung befürchten die Personen 4 und 11, wobei die Person 11 die Aufarbeitung der Daten mit Statistiken erklärt, sich jedoch unsicher ist, ob sämtliche Daten von unterschiedlichen Personen aufschlussreich sein können.³⁴⁹ Während sich die Person 6 überhaupt nicht vorstellen kann, welche Folgen die Datenspeicherung für uns haben kann, denkt die Person 7 vor allem an die Ausnutzung der Daten und der Kontakte wegen wirtschaftlicher Anreize.³⁵⁰

10.7. Kategorie 7: Mögliche Folgen von Big Data

Auf die Frage, ob sie sich aufgrund der Datenspeicherung auch schon überlegt haben, einen Dienst zu löschen, sprach die Person 6 das entscheidende Thema an. Sie sagte, sie wisse nicht, welche Nachteile dies habe, wenn jemand Daten über jemand anderen hat.³⁵¹ Die Person 7, die selbst schon Erfahrungen in diesem Bereich gemacht hat, hat sich zwar darüber Gedanken gemacht, ebenso wie Person 5, die Apps ablehnt, die einen zu großen Datenzugriff verlangen, aber effektiv Dienste bzw. Apps gelöscht haben nur die Personen 3 und 8.³⁵² Die Person 3 besitzt aus eben diesem Grund nicht so viele Apps³⁵³ und Person 10 besitzt als Schutz eine Viren App. Wenn diese App meldet, dass eine andere App unnütze Zugriffe besitzt und viele Daten herunterlädt, dann löscht sie diese App auch.³⁵⁴ Sich Gedanken darüber gemacht, ob sie einen Dienst löschen, haben sich hingegen die Personen 1, 2, 4, 9 und 11 noch nie.³⁵⁵

Sehr genau wissen die UntersuchungsteilnehmerInnen, was passieren müsste, dass sie sich von einem Dienst wirklich abmelden würden. Sieben Personen nennen als Grund die Veröffentlichung von persönlichen Daten³⁵⁶, vier Personen hingegen nennen eine

³⁴⁷ Vgl. Interview 3: Z 202; Interview 5: Z 245; Interview 9: Z 215-216

³⁴⁸ Vgl. Interview 3: Z 202-219

³⁴⁹ Vgl. Interview 11: Z 219-227

³⁵⁰ Vgl. Interview 6: Z 245; Interview 7: Z 274-275

³⁵¹ Vgl. Interview 6: Z 253-254

³⁵² Vgl. Interview 7: Z 220-221; Interview 5: Z 249-251; Interview 3: Z 222-224; Interview 8: Z 220-223

³⁵³ Vgl. Interview 3: Z 220-223

³⁵⁴ Vgl. Interview 10: Z 214-216

³⁵⁵ Vgl. Interview 1: Z 182-183; Interview 2: Z 174; Interview 4: Z 247; Interview 9: Z 218-219; Interview 11: Z 234

³⁵⁶ Vgl. Interview 1: Z 186-187; Interview 2: Z 177-178; Interview 3: Z 239-241; Interview 4: Z 249-250; Interview 7: Z 293-294; Interview 9: Z 221-222; Interview 11: Z 245-248

verletzte oder ungeschützte Privatsphäre.³⁵⁷ Die Person 8 spricht hier übertriebene Kosten als Grund an.³⁵⁸ Allein die Person 6 hat über diese Möglichkeit noch nie nachgedacht.³⁵⁹ Auf die Frage, wie sich die TeilnehmerInnen in Zukunft vor der Datenspeicherung schützen wollen, antwortet die Person 8 sehr ausführlich. „Mich informieren vor allem. Man bekommt ja viel mit in den Medien. Ganz wichtig ist auf Facebook immer wieder kontrollieren, was ist jetzt neu, auch durchlesen dann. Da nehme ich mir schon oft die Zeit, das durchzulesen, wenn es neue Einstellungen gibt. Dann schau ich auch, ob sich da etwas in meiner Sicherung verändert hat oder hat sich das nun alles veröffentlicht, so zu sagen.“³⁶⁰ Bei aktuellen Themen sucht sie auch häufig in Computerportalen nach Antworten.³⁶¹ Das Bedürfnis sich zu schützen, erklärt der/die TeilnehmerIn damit, dass er/sie selbst bestimmen möchte, was andere Personen über ihn/sie wissen sollen und was nicht. Diese Entscheidung überlässt er/sie nicht einer sozialen Plattform.³⁶² Informieren möchte sich auch die Person 6, wobei sie hier nicht die Medien als Ratgeber sucht, sondern sich lieber die Tipps der Autorin nach dem Interview einholt.³⁶³ Die Datenschutzrichtlinien durchzulesen, nehmen sich die Personen 2, 3, 5, 7, 8 und 9 vor.³⁶⁴ Wobei dies bei manchen mehr wie eine Idee klingt, als ein konkretes Ziel. Der/die Befragte 2 spricht dabei einen wichtigen Aspekt an, nämlich, dass man diese erst einmal verstehen muss.³⁶⁵ Den Befragten 4 und 10 sind die Datenschutzrichtlinien zu lang, als dass es für sie in Frage käme, diese durchzulesen, die Person 4 möchte sich aber schützen, indem sie die Verbindung mit dem Internet verweigert.³⁶⁶ Auch die Person 10 ist aufgeschlossen gegenüber einer besseren Möglichkeit ihre Daten zu schützen, Voraussetzung ist dabei jedoch, dass es einfach und unkompliziert ist.³⁶⁷ Die Person 1 möchte sich einfach durch eine geringere Preisgabe ihrer eigenen Daten schützen und hier auch kontrollieren, welche Zugriffe die Apps sich erlauben möchten.³⁶⁸ Allein die Person 11 hat im Moment kein spezielles Interesse daran, ihre Daten zu schützen. Der Grund dafür liegt in ihrer Einstellung, dass persönliche Daten von unauffälligen, „normalen“

³⁵⁷ Vgl. Interview 5: Z 274-275; Interview 8: Z 239-246; Interview 10: Z 223-228; Interview 11: Z 259-262

³⁵⁸ Vgl. Interview 8: Z 235-238

³⁵⁹ Vgl. Interview 6: Z 260

³⁶⁰ Interview 8: Z 256-260

³⁶¹ Vgl. Interview 8: Z 267-269

³⁶² Vgl. Interview 8: Z 262-264

³⁶³ Vgl. Interview 6: Z 263

³⁶⁴ Vgl. Interview 2: Z 180; Interview 3: 246-247; Interview 5: Z 279-279; Interview 7: Z 296; Interview 8: Z 257-260

³⁶⁵ Vgl. Interview 2: Z 180-181

³⁶⁶ Vgl. Interview 4: Z 252-253

³⁶⁷ Vgl. Interview 10: Z 237-238

³⁶⁸ Vgl. Interview 1: Z 189-190

Personen keinen Wert besitzen.³⁶⁹ Dies zeigt im Grunde aber auf, dass sie die Gefahren, welche durch eine massive Datensammlung und –Analyse ausgehen können, nicht verstanden hat.

Die Vorstellungen darüber, wie unser Leben mit den Technologien in Zukunft aussehen wird, gehen weit auseinander. Die Personen 1, 2, 3 und 9 denken, dass das Handy noch mehr genutzt wird als heute, dass alles noch mehr verstrahlt und unsicherer wird, ergänzt die Person 3.³⁷⁰ Eine verstärkte Nutzung mit geringerem Schutz vermutet auch die Person 6³⁷¹. Dass es in Zukunft eine neue Technologie gibt, die wir benutzen, das vermuten die Personen 5, 7, 8 und 10.³⁷² Aber auch hier unterschieden sich die Meinungen. Während die Person 5 von einem Höhepunkt der Technologiebenutzung ausgeht: „steigern oder so, dass die Leute noch mehr Handys und Tablets haben, das denke ich nicht“,³⁷³ vermutet die Person 10 eine noch stärkere Überwachung, als es heute schon der Fall ist.³⁷⁴ Die Person 4 befürchtet, dass die Datenspeicherung komplett aus den Rudern läuft und irgendwann auch Personen zu Daten kommen können, die sie gar nicht mal besitzen dürften.³⁷⁵ Die Person 11 denkt, dass sich nicht viel ändern wird, dass es eingepflanzte Chips oder dergleichen geben könnte, hält der/die TeilnehmerIn für unrealistisch.³⁷⁶ Das Prinzip, dass jeder mit jedem durch die Technologien verknüpft ist, wird laut ihrer Meinung aber erhalten bleiben.³⁷⁷

Das Szenario zum Thema *Bewegungsprognosen* hält die Person 4 für unrealistisch, die Person 1 ist sich unsicher und alle weiteren Befragten sehen es als realistisch an. Als Grund geben die TeilnehmerInnen 1, 3, 5, 6, 7, 8 und 10 die Standortsuche, bzw. die Ortung des Handy an, die Person 2 denkt im ersten Moment an die Suchverläufe im Internet und die Personen 9 und 11 erwähnen die Möglichkeit der Analyse des vergangenen Verhaltens, um den Aufenthaltsort in der Zukunft zu bestimmen. Die Person 3 verweist darauf, dass das System unterschätzt wird. Es sei leichter auf Sachen

³⁶⁹ Vgl. Interview 11: Z 267-272

³⁷⁰ Vgl. Interview 1: Z 192; Interview 2: Z 183; Interview 3: Z 155-156; 262-263; Interview 9: Z 236

³⁷¹ Vgl. Interview 6: Z 266-268

³⁷² Vgl. Interview 5: Z 282; 284; Interview 7: Z 299-300; Interview 8: Z 274-275; Interview 10: Z 245-246

³⁷³ Interview 5: Z 284-285

³⁷⁴ Vgl. Interview 10: Z 246-247

³⁷⁵ Vgl. Interview 4: Z 255; 258.259

³⁷⁶ Vgl. Interview 11: Z 285-288

³⁷⁷ Vgl. Interview 11: Z 289-290

zuzugreifen, als wir meinen, sagt sie.³⁷⁸ Auf die spezielle Nachfrage, ob die Befragten auch denken, dass dies allein mit den Informationen der engsten Facebook-Freunde möglich sei, äußern die Person 2 und 10, dass sie das für unrealistisch halten³⁷⁹, auch die Person 11 äußert hinsichtlich dieser Möglichkeit Zweifel.³⁸⁰ Die Person 4 hält es für möglich³⁸¹ und die Person 5 ist sich sicher, dass die Erstellung eines Bewegungsprofils mit den Informationen der Facebook-Freunde möglich ist.³⁸² Der gleichen Meinung ist die Person 6, wobei sie nicht erklären kann, wie das funktioniert, sie gibt aber an, bereits davon gehört zu haben, dass durch die Facebook-App dies ermittelt werden kann.³⁸³ Auch die Person 7 hält diese Möglichkeit für realistisch, durch das Zusammenführen von Informationen³⁸⁴. Die Person 8 hat von dieser Möglichkeit bereits gehört.³⁸⁵

Die Auswertung des Szenarios der *Verbrechensvorhersage* durch die Polizei, welches bereits in den USA getestet wurde, fanden die Personen 1, 2, 3, 4, 6 und 8 als unrealistisch. Als Gründe gaben die Personen 2 und 8 an, dass dies viel zu viel Arbeit wäre, jeden einzelnen Bürger zu überwachen, die Personen 3 und 4 sind der Meinung, dass dies bereits umgesetzt würde, wenn dies möglich sei. Auf die gezielte Nachfrage, wie realistisch die TeilnehmerInnen es halten, dass man aus den Verbrechensdaten der Vergangenheit die Verbrechen in Zukunft mit Wahrscheinlichkeit vorhersagen kann, fanden die Befragten 1, 2, 6 und 8 unrealistisch. Die Personen 5, 7, 9, 10 und 11, die hingegen das Szenario als realistisch einstufen, sind auch der Meinung, dass die Verbrechensvorhersage mit Hilfe vergangener Verbrechen möglich sei. Sie begründen ihre Meinung mit Zusammenhängen³⁸⁶, sowie damit, dass sie es für wahrscheinlich halten, dass wenn an einem Ort schon mal ein Verbrechen stattfand, dies wieder dort stattfinden kann.³⁸⁷

Die Auswertung des Szenarios der *Vorhersage von Schwangerschaften und den ungefähren Geburtstermin* ergab ein ähnliches Verhältnis wie beim Verbrechensszenario.

³⁷⁸ Vgl. Interview 3: Z 272-273

³⁷⁹ Vgl. Interview 2: Z 197; Interview 10: Z 273-277

³⁸⁰ Vgl. Interview 11: Z 315

³⁸¹ Vgl. Interview 4: Z 271

³⁸² Vgl. Interview 5: Z 321-324

³⁸³ Vgl. Interview 6: Z 286-295

³⁸⁴ Vgl. Interview 7: Z 322-327

³⁸⁵ Vgl. Interview 8: Z 296-298

³⁸⁶ Vgl. Interview 5: Z 351; Interview 7: Z 357-358; Interview 11: Z 337-341

³⁸⁷ Vgl. Interview 5: Z 351; Interview 7: 361-363; Interview 9: Z 295-296; Interview 10: Z 300-312; Interview 11: Z 347-349

Die Mehrheit der Befragten hält dies für unrealistisch, weil sie denken, dass es nicht rückschließbar ist und durch nicht Preisgabe von persönlichen Daten dies nicht möglich sei. Die Person 4 ist sich als einzige unsicher. Sie ist der Meinung, dass die Vorhersage mit einer gesunden Ernährung einhergeht. Da sich aber nicht nur Schwangere gesund ernähren, ist sie sich doch unsicher. Vollkommen überzeugt, dass dies möglich ist, sind sich die Befragten 5, 8, 9 und 11. Alle begründen dies durch Zusammenhänge von Produktvorlieben von Schwangeren und den individuellen Einkaufsverhalten der betreffenden Frau.³⁸⁸ Auch die Wahrscheinlichkeitsberechnung des Geburtstermins finden die Personen 8, 9 und 11 realistisch.³⁸⁹

Interessant ist, dass das Szenario zum Thema *Homosexualität* fast alle Beteiligten als realistisch einstufen, außer der Person 2, die es zuerst für unrealistisch hält, anschließend es aber doch für möglich hält, durch die Kombination von Daten.³⁹⁰ Alle anderen Befragten führen das auf das Verhalten des Homosexuellen zurück, sowie auf die Kombination seines Verhaltens oder anderen Daten. Es wird beobachtet, dass die TeilnehmerInnen dabei häufig auch auf eigene Erfahrungen zurückgreifen,³⁹¹ wie zum Beispiel der/die Befragte 4: „aber das sieht man ja selbst auch.“³⁹²

Das Szenario zum Thema *Überwachung der Kreditinstitute* finden alle Befragten realistisch, und geben als Grund die finanzielle Absicherung des Kreditinstitutes an. Die Person 10 spricht dabei einen wichtigen Aspekt an: „solange die Kosten von der Kontrolle der Person nicht die möglichen Schäden übersteigen.“³⁹³ Vergleiche mit dem Arbeitsmarkt und der Kontrolle des Arbeitgebers stellen dabei die Personen 5, 6 und 11 an. Die Personen 4 und 6 sind der Meinung, dass das heute noch nicht praktiziert wird.

Bei der Auswertung des Szenarios zum Thema *Überprüfung des Gesundheitszustandes* mittels Gesundheit-App ist zu beobachten, dass dies alle Beteiligten, außer der Person 11 für realistisch halten. Als Motiv werden hier wiederum finanzielle Gründe geäußert. Die Person 11 hingegen meint, dass diese Kontrolle die BürgerInnen selbst nicht zulassen

³⁸⁸ Vgl. Interview 5: Z 370-373; Interview 8: Z 324-327; Interview 9: Z 304-305; Interview 11: Z 362-369

³⁸⁹ Vgl. Interview 8: Z 335-337; Interview 9: Z 311-313; Interview 11: Z 377-378

³⁹⁰ Vgl. Interview 2: Z 229-230

³⁹¹ Vgl. Interview 5: Z 387-391; Interview 6: Z 351-352; Interview 7: Z 388; Interview 8: Z 350-351; Interview 11: Z 412-413

³⁹² Interview 4: Z 313

³⁹³ Interview 10: Z 371-372

würden.³⁹⁴ Auch die Person 10 ist dem Szenario gegenüber skeptisch und äußert Zweifel, ob diese App wirklich viel Sinn macht, weil sie vermutet, dass die App nur einzelne Daten erhält und somit ein ungenaues Bild aufzeigen würde.³⁹⁵

Sehr interessante Ergebnisse liefert die Auswertung des Szenarios zum Thema *Kommunikationsüberwachung*. Die Personen 1, 3, 5, 7, 9, 10 und 11 denken, dass dieses Szenario realistisch ist, während die Personen 2, 4 und 8 dies verneinen. Die Person 6 ist sich unsicher. Interessant ist dabei, dass die Person 11 zwar der Meinung ist, dass Einreisende überprüft werden, aber jene Personen, die nur als Urlaubsgäste in ein Land einreisen von dieser Kontrolle ausgeschlossen sind, weil es ein zu großer Aufwand wäre, jeden einzelnen zu überprüfen.³⁹⁶ „Außer es ist ein mathematisches Programm, das alles durchsucht, aber das kann ich mir nicht vorstellen. Da würden auch nur Missverständnisse rauskommen, wahrscheinlich. Deswegen: Kurzfristig gesehen, wenn man nur kurzfristig einreist, ist da nichts, von mir aus gesehen. Das wäre meiner Meinung zu aufwändig.“³⁹⁷ Dass es an den technischen Möglichkeiten der Überprüfung scheitert, denken außerdem auch die Befragten 2, 4, 6 und 8. Von jenen TeilnehmerInnen, die dieses Vorgehen als realistisch einstufen, wird häufig das Motiv des eigenen Schutzes genannt. Auch wird Amerika in diesem Zusammenhang oft erwähnt. Eine sehr umfassende Antwort gibt hier die Person 10, welche auch die aktuellen Geschehnisse mit berücksichtigt.³⁹⁸ Einen entscheidenden Aspekt zu diesem Thema nennt die Person 3: „Ja ich denke schon, dass wir das nicht so bewusst wahrnehmen, aber ich denke schon, dass es so ist, ja.“³⁹⁹

Die abschließende Frage, ob die Befragten der Meinung sind, dass man das Verhalten der Zukunft aus dem Verhalten der Vergangenheit mit einer gewissen Wahrscheinlichkeit vorhersagen kann, beantworteten alle mit ja. Die Person 8 geht hier sehr genau auf die einzelnen Faktoren ein, welche man stets berücksichtigen muss, weil es im Leben natürlich immer Veränderungen geben kann.⁴⁰⁰ Die Person 1 spricht dabei einen

³⁹⁴ Vgl. Interview 11: Z 443-449

³⁹⁵ Vgl. Interview 10: Z 387-388; 392-394

³⁹⁶ Vgl. Interview 11: Z 477-479

³⁹⁷ Interview 11: Z 484-487

³⁹⁸ Vgl. Interview 10: 415-421

³⁹⁹ Interview 3: Z 406-407

⁴⁰⁰ Vgl. Interview 8: Z 425-431

wichtigen Umstand an, nämlich, dass dabei nicht die Menge an preisgegebenen Daten entscheidend ist, sondern auch wenig Daten wiederum Informationen liefern.⁴⁰¹

11. Beantwortung der Forschungsfragen

Forschungsleitende Frage 1: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über Big Data im Allgemeinen?

Insgesamt wissen viele jungen Erwachsene der Untersuchungsreihe sehr wenig über den Begriff oder die Bedeutung von Big Data Bescheid. Viele bringen damit das Thema Datenschutz in Verbindung.

Forschungsleitende Frage 2: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über die Datenspeicherung im Zusammenhang mit der Nutzung von Smartphones?

Die UntersuchungsteilnehmerInnen wissen zum Teil, dass manche ihrer Daten am Smartphone von Unternehmen mitgelesen und gespeichert werden können. Dieses Wissen tritt bei der Nutzung des Smartphones jedoch in den Hintergrund. Sie sind sich bewusst, dass sie selbst für die Sicherheit ihrer Daten verantwortlich sind und durch die Zustimmung der Datenschutzrichtlinie, Erlaubnisse u.a. zur Datenspeicherung erteilen. Wobei hier das Wissen und die dementsprechende Umsetzung nicht im Gleichgewicht stehen. Die Befragten sind sich größtenteils nicht bewusst, dass sie diese Speicherung auch kontrollieren können.

Forschungsleitende Frage 3: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über die Auswertung und Analyse ihrer Daten, die sie bei der Nutzung ihres Smartphones generieren?

Die jungen Erwachsenen wissen, dass die Datenspeicherung dazu verwendet wird, um personalisierte Werbung zu erstellen. Dass die Daten dazu, nach der Speicherung ausgewertet und analysiert werden, sprechen nur wenige an. Nur sehr informierte

⁴⁰¹ Vgl. Interview 1: Z 318-321

Personen wissen, dass die Daten mit Hilfe von Programmen analysiert werden und somit auch für andere Zwecke ausgewertet werden können.

Forschungsleitende Frage 4: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über die Vorhersagbarkeit ihres Verhaltens?

Junge Erwachsene der Untersuchungsreihe sind der Meinung, dass man das zukünftige Verhalten einer Person aus der Analyse ihres vergangenen Verhaltens vorhersagen kann, wobei hier die Charaktereigenschaften und Vorlieben der Person berücksichtigt werden. Die meisten TeilnehmerInnen wissen hingegen nicht, dass es für Vorhersagen ihres eigenen Verhaltens nur sehr wenige persönliche Daten braucht, wenn genügend Daten von anderen Personen zur Verfügung stehen. Auch ist ihnen nicht bewusst, dass auch das Nicht-Teilnehmen an der Datenpreisgabe schon viel über einen selbst verrät.

Forschungsleitende Frage 5: Was wissen junge Erwachsene im Alter zwischen 18 und 24 Jahren über die möglichen Folgen von Big Data in der Zukunft?

Junge Erwachsene wissen, dass die Datenspeicherung in erster Linie für die Erstellung von personalisierter Werbung genutzt wird, aber auch, dass sie zur Überwachung führen kann und eine eingeschränkte Privatsphäre die Folge sein kann.

Jene Szenarien von Folgen einer Big-Data Zukunft, welche die Untersuchungspersonen mit konkreten eigenen Erlebnissen oder Medieninhalten verbinden können, werden größtenteils realistisch eingestuft, weil die wirtschaftlichen Mechanismen dahinter erkannt werden. Szenarien, welche sie nicht an ihre bisherigen Informationen, wie eigenen Erfahrungen oder Medieninhalte anknüpfen können, werden vermehrt als unrealistisch eingestuft.

Grundsätzlich herrscht nur ein sehr geringes Bewusstsein vor, dass jeder einzelne sich durch einen vorsichtigen, verantwortungsvollen Umgang mit den persönlichen Daten bis zu einem gewissen Punkt schützen kann.

12. Interpretation und Diskussion der Forschungsergebnisse

Insgesamt haben die jungen Erwachsenen heute kein ausreichendes Fakten- und Kontextwissen über Big Data und seine Folgen. Es ist zwar bei vielen das Bewusstsein und ein Ansatz von Wissen vorhanden, nur leider in einer unzureichenden Form, um sich selbst vor möglichen negativen Auswirkungen der Datenanalyse zu schützen. Relevant, besonders für diese Untersuchung, ist die Kombination der gegebenen Antworten mit der Nutzung von Informationsangeboten. Jene Personen, die aussagten, dass sie Informationen aus Medien nutzen oder gezielt danach suchen, konnten im Interviewverlauf die Fragen ausführlicher und zum Teil treffender beantworten, als jene, die Informationsangebote von Medien meiden oder nicht beachten.

Im Allgemeinen kann man festhalten, dass die Antworten zum Thema Datenschutz sehr unterschiedlich ausgefallen sind. Manche TeilnehmerInnen besitzen ein gutes, andere ein unzureichendes Wissen zum Thema. Die eigene Einschätzung, wie gut man sich beim Datenschutz auskennt, entspricht dabei manchmal nicht dem geäußerten Wissen. Eine sehr gute Bewertung in diesem Bereich traut sich keinE UntersuchungsteilnehmerIn zu. Dies kann auch damit in Verbindung gebracht werden, dass das Thema Datenschutz sehr umfangreich und tiefläufig ist, und eine intensive Auseinandersetzung mit dem Thema notwendig ist, um sich ausreichend zu informieren. Vom Begriff Datenschutz haben die jungen Erwachsenen unterschiedliche Auffassungen. Er wird mit einem Schutz der persönlichen Daten vor Veröffentlichung, vor der Weitergabe an Dritte und mit einer Zugriffsverweigerung assoziiert. Eine Datenschutzrichtlinie ist hingegen, außer einer Person, allen UntersuchungsteilnehmerInnen ein Begriff, womit auch das Bewusstsein einhergeht, schon selbst eine Datenschutzrichtlinie unterzeichnet zu haben. Auf die Frage, was in einer Datenschutzrichtlinie geregelt wird, herrscht bei sechs Personen Unsicherheit. Nur vier Personen geben eine ausführliche Antwort über den Inhalt und Nutzen der Datenschutzrichtlinie. Die jungen Erwachsenen wissen zwar sehr gut darüber Bescheid, wo sie sich über die geltenden Datenschutzbestimmungen informieren könnten, aber das Interesse sich die Datenschutzrichtlinien durchzulesen, ist sehr gering. Neun Personen haben sich noch nie eine Datenschutzrichtlinie durchgelesen. Dies hängt vor allem mit der Länge und zum Teil schwer verständlichen Formulierung der Richtlinie zusammen. Es ist hier ein Ungleichgewicht zwischen gewünschtem Zustand und eigenem Aufwand feststellbar. Zum einen wird betont, dass der Schutz der eigenen Daten einen sehr hohen Stellenwert hat, andererseits wird es aber unterlassen, sich die Datenschutzbestimmungen durchzulesen und/oder sich über den Schutz zu informieren.

Eine Folge ist, dass bei der Nachfrage, auf welche Daten ihre Apps zugreifen können, zum Teil unsichere bzw. unvollständige Antworten gegeben werden. Nur zwei UntersuchungsteilnehmerInnen können hier sichere und genaue Antworten geben. Auffallend ist, dass jene UntersuchungsteilnehmerInnen, die sich in diesem Bereich informieren, treffendere und präzisere Antworten geben. Besonders interessant ist der Unterschied zwischen dem bloßen Faktenwissen und dem bewussten Umgang während der Smartphonebenutzung. Während manche TeilnehmerInnen relativ gut über das Szenario des Datenzugriffes Bescheid wissen und auch erklären können, zehn Untersuchungspersonen sind von der Möglichkeit des Fremdzugriffes überzeugt, ist die Hälfte der Befragten bei der anschließenden Frage, wie es mit dem Datenzugriff von Apps auf ihr eigenes Smartphone bestellt ist entweder unsicher, oder sogar erschrocken. In dieser Hinsicht korreliert das Bewusstsein des eigenen Handelns am Smartphone nicht mit dem theoretischen Wissen.

Bei der Frage, wie gut die eigenen Daten geschützt sind, beantwortet dies nur die Person 8 mit gut. Vier Personen sind sich unsicher, 5 Personen denken eher nicht gut. Nur eine Person gibt an, dass sie weiß, dass ihre Daten nicht gut geschützt sind. Das Bewusstsein, dass sie eigenhändig die Sicherheit ihrer Daten bestimmen und sie selbst die Erlaubnis zum Datenzugriff erteilen, ist jedoch vorhanden. Ob diese Erlaubniserteilung den SmartphonebesitzerInnen stets bewusst ist, daran zweifeln auch viele InterviewpartnerInnen, eben weil die Datenschutzrichtlinien nur minimale Beachtung finden.

Als Grund, wieso Apps Datenzugriff brauchen, nennen die Befragten in erster Linie die Ausführung von Funktionen, wobei ihnen auch bewusst ist, dass die Finanzierung durch Werbungen, sowie Datenverkauf ein Motiv der Unternehmen ist. Die TeilnehmerInnen wissen, dass Unternehmen mit Hilfe der Datenspeicherung personalisierte Werbung erstellen können. Einzelne denken dabei auch an eine Erpressung, Ausnutzung der Daten oder Überwachung. Die UntersuchungsteilnehmerInnen wissen demnach, dass ihre Daten weiterverarbeitet werden können, wie genau dies geschieht, erklärt allerdings nur die Person 10 sehr ausführlich. Die Ergebnisse der DIVISI-Studie 2013 über das eigene Vertrauen, Risiken online gut einschätzen zu können, können mit den Ergebnissen dieser Studie nur ansatzweise verglichen werden.

Als Folge befürchten manche eine eingeschränkte Privatsphäre und eine Überwachung der eigenen Person, womit auch das eigene Verhalten verändert wird. Im Hinblick auf ein

neues Maß an Privatsphäre, das die DIVISI-Studie 2014 anspricht, kann auch auf die Ergebnissen dieser Untersuchung Bezug genommen werden. Die InterviewpartnerInnen streben danach, selbst zu bestimmen was andere über sie selbst wissen sollen oder nicht und welche Information effektiv verbreitet werden soll. Diesen Sachverhalt spricht explizit die Person 8 im Interview an, womit sie diese Entscheidung nicht freiwillig Unternehmen oder sozialen Netzwerken übergibt. Die Risikowahrnehmung der Weitergabe von privaten Daten an Dritte, welche bei der DIVISI-Studie 2014 bei 55 Prozent lag, zeigte sich auch in dieser Untersuchung. Eine Weitergabe von persönlichen Daten oder eine verletzte Privatsphäre wäre beinahe für alle Untersuchungsteilnehmerinnen der ausschlaggebende Grund eine App zu löschen. Die Privatsphäre und der Umgang mit privaten Informationen wird in diesem Kontext neu interpretiert. So wie die DIVISI-Studie 2014 zeigt, herrscht online eine ständige Kosten-Nutzen-Abwägung, ob persönliche Inhalte veröffentlicht bzw. geteilt werden oder nicht. Der Schutz der eigenen Daten ist den jungen Erwachsenen der Untersuchung allgemein sehr wichtig, besonders eine Veröffentlichung persönlicher Daten wäre für die Mehrheit ein Grund einen Dienst zu kündigen. Bisher haben jedoch weniger als die Hälfte der TeilnehmerInnen eine App nach der Installation wieder gelöscht. Die Motive liegen dafür zum einen bei übertriebener Datenspeicherung, also auch Nicht-Benutzung der App, sowie Unsicherheit. Für die Zukunft sehen einige das Durchlesen der Datenschutzrichtlinie als Möglichkeit, sich vor ungewollter Datenspeicherung zu schützen. Allgemein wird aber mittgeteilt, dass die Datenschutzrichtlinien oft zu lang und zum Teil auch unverständlich verfasst sind. Andere wollen in Zukunft mehr darauf achten, auf welche Daten Apps Zugriff haben, bzw. die Privatsphäreinstellungen prüfen, um negativen Folgen vorzubeugen.

Im Hinblick auf das Strukturwissen ist zu betonen, dass niemand der elf UntersuchungsteilnehmerInnen alle Szenarien korrekt einschätzen konnte. Verbreitet ist das Wissen, dass Daten gespeichert und dazu verwendet werden können um eine personalisierte Werbung zu erstellen. Auch die Profilerstellung durch Werbetreibende wird öfters genannt. Eine Datenspeicherung ist für die Unternehmen auch wirtschaftlich rentabel. Welche zukünftige Auswirkung die heutige Datenspeicherung aber noch haben kann, wissen nur sehr wenige. Zu beobachten ist hier, dass es oft am technischen Know How, sowie dem Durchblicken finanzieller Mechanismen fehlt, das, wie schon Constanze Kurz und Frank Rieger erklären, notwendig ist, um die daraus resultierende Motivation

der Menschen zu verstehen. Sehr deutlich sprechen dies die Personen 1, 3, 6 und 11 in ihrem Interview an, bei dem sie angeben, nicht zu verstehen, welchen Nutzen ihre Daten für andere haben können, da sie selbst ja nur „normale“ Leute sind. Ein sehr ausgeprägtes Allgemeinwissen besitzt die Person 10, die die gesellschaftlichen Zusammenhänge versteht und auch auf die Machtverhältnisse und das staatliche Streben nach Kontrolle der Bevölkerung eingeht. Auch die Person 5 erklärt die Zusammenhänge treffend, bedingt durch ihr Studium besitzt sie das nötige technische Wissen. Die Folge des fehlenden Kontextwissens ist, dass rund die Hälfte der Befragten nicht weiß, dass ihre Daten auch für Analysen außerhalb des Werdebereiches nützlich sein können. Die einzelnen Szenarien einer möglichen Big Data Zukunft zeigen sehr schön, dass viele Personen der Meinung sind, dass nur unter Preisgabe von persönlichen Daten, Rückschlüsse auf ihre Person möglich seien. Die Verknüpfung von scheinbar irrelevanten Daten dahingehend, dass auch bei einer nicht Preisgabe von persönlichen Daten, Rückschlüsse auf die eigene Person möglich sind, scheint hier - zumindest im ersten Moment - zu komplex. Veranschaulicht wird das durch die Antworten auf die Szenarien der Bewegungsprognose, der Verbrechensvorhersage, der Vorhersage einer Schwangerschaft sowie des Geburtstermins und der Kommunikationsüberwachung. Das Szenario zum Thema Bewegungsprognosen halten neun Personen für realistisch. Als Möglichkeiten werden hier die Standortsuche des Handys, die Kontrolle der Internetsuchverläufe, sowie die Analyse des vergangenen Verhaltens genannt. Die spezielle Methode der Analyse mittels Facebook-Kontakten scheint dabei fünf Personen realistisch, zwei Personen halten dieses Verfahren jedoch für nicht möglich, eine ist sich unsicher. Das Szenario der Verbrechensvorhersage zeigt ein ähnliches Bild. Sechs Personen halten es für unrealistisch, wenn keine persönlichen Daten vorliegen. Auch wenn die Methode der Analyse vergangener Verbrechen erklärt wird, ändern sie ihre Meinung nicht. Jene Personen, die das Szenario für realistisch einstufen, stimmten auch der Analyse vergangener Verbrechen zu.

Beim Szenario der Vorhersage einer Schwangerschaft und des Geburtstermins sind sechs TeilnehmerInnen der Meinung, dass dies nicht möglich sei, ohne persönliche Angaben der Frau zu haben. Eine Person ist sich unsicher, vier Personen halten dieses Szenario für realistisch. All jene, die es für realistisch einstufen, gehen dabei auf Zusammenhänge zwischen dem Einkaufsverhalten von schwangeren Frauen und einer unbekannten Frau ein. Das bei manchen Personen fehlende technische Verständnis zeigt sich besonders gut beim Szenario der Kommunikationsüberwachung. Während sieben Personen dies für

realistisch halten, sehen drei Personen es als unrealistisch, eine Person ist sich unsicher. Jene, die Unsicherheit oder eine Unwahrscheinlichkeit geäußert haben, können es sich nicht vorstellen, dass dies technisch möglich sei. Das Kosten-Nutzen-Verhältnis zwischen Überwachung und tatsächlicher Bedrohung wäre bei einer von Personen durchgeführten Überwachung nicht ausgewogen. Des weiteren ist dieses Szenario auch ein gutes Beispiel dafür, dass die Kommunikationsüberwachung nur in einem geringen Ausmaß wahrgenommen wird. Viele Personen assoziieren eine Überwachung mit verdächtigen oder auffälligen Persönlichkeiten und fühlen sich daher weder überwacht, noch angesprochen, obwohl dies natürlich nicht der Fall ist.

Anders verhält es sich beim Szenario zum Thema Sexualleben. Hier haben die jungen Erwachsenen eigene Erfahrungen, die sie in ihre Bewertung mit einfließen lassen. Ähnliche Erfahrungen oder Berichterstattungen zu einem Thema lassen die UntersuchungsteilnehmerInnen die dahinterstehenden Motive erkennen. Die Einschätzung der Szenarien zur Überwachung der Kreditinstitute, sowie zur Überprüfung des Gesundheitszustandes mittels App sind dementsprechend positiv. Die abschließende Frage, ob die jungen Erwachsenen der Meinung sind, dass man aus dem Verhalten der Vergangenheit das Verhalten in der Zukunft mit einer gewissen Wahrscheinlichkeit vorhersagen kann, bejahten alle Untersuchungspersonen. Sie begründeten dies vor allem mit den eigenen Erfahrungen und der Tatsache, dass sich ein Mensch für gewöhnlich in seinen Verhaltensweisen nicht von heute auf morgen ändert. Ob die UntersuchungsteilnehmerInnen nun auch das Bewusstsein erlangt haben, dass die eigenen Verhaltensweisen, auch am Smartphone, viel über unsere eigene Zukunft aussagen und sich daher bewusst in einer bestimmten Art verhalten, muss an dieser Stelle offen bleiben.

Das Strukturwissen muss noch stark verbessert werden, u.a. mit Hilfe medialer Berichterstattungen. Aus den Interviews ist deutlich zu erkennen, dass die Personen über Themen, die viel Beachtung in den Medien gefunden haben, besser Bescheid wussten als über nicht beachtete Themen seitens der Medien. Das Ergebnis der Divisi-U-25-Studie, dass eine hohe Präsenz von Themen in medialen Diskursen sich erkennbar auf die Wissensbestände von jungen Erwachsenen niederschlägt, kann in dieser Studie auch bestätigt werden. Auch die Ergebnisse der Studie von Yong Jin Park et al. *Affect, cognition and reward: Predictors of privacy protection online*⁴⁰² sind für diese Studie

⁴⁰² Vgl. Yong Jin Park, et al., 2012. S. 1019-1027.

treffend. Wer mehr Medien und spezielle Informationen zum Thema Datenschutz nutzt, kennt sich besser aus, weiß in Folge dessen von den Gefahren und schützt sich daher besser. Besonders die Personen 5, 8 und 10 können hier als Beispiel genannt werden.

Da die Befragten mit großer Mehrheit angaben, dass sie sich die Datenschutzrichtlinien nie durchlesen, kann davon ausgegangen werden, in Anlehnung an die Studie von Kuang-Wen Wu et al. *The effect of online privacy policy on consumers privacy concern and trust*,⁴⁰³ dass sich ihr Verhalten in der Preisgabe ihrer Daten oder der Installation von übertrieben datenspeichernden Programmen (Apps) verändern würde. Der Schutz der eigenen Daten ist nämlich fast allen Beteiligten ein großes Anliegen. Das Wissen darüber ist aber nicht so ausgeprägt, wie es für einen guten Schutz erforderlich wäre. Manche Befragten wissen zwar, dass Apps auf ihre persönlichen Daten am Smartphone zugreifen können, aber viele meinen, dass ihre Fotos etc. vor jeglicher Einsichtnahme durch andere geschützt seien, bedenken dabei aber nicht, dass sie dazu sogar selbst die Erlaubnis erteilt haben. Die DIVISI-Studie 2013 zeigt, dass nur vier Prozent der gesamten Internetnutzer bewusst wahrgenommen haben, dass sich fremde Personen Zugang zum eigenen Computer verschaffen konnten. Dem entgegen sprechen jedoch die Zahlen des BSI, welche im Jahr 2013 innerhalb von 3 Monaten rund 250.000 Identitätsdiebstahle belegen.⁴⁰⁴

Verschiedene Studien berichten, dass Jugendliche und junge Erwachsene ein Bewusstsein für Datenschutz besitzen und dem Schutz ihrer Daten auch Wichtigkeit beimessen, doch bedeutet dies noch nicht, dass sie sich auch ausreichend vor Big Data – Folgen schützen. Wie Marwick und Boyd bereits festhalten, ist das tiefgehende Verständnis des Kontextes, in dem die eigenen Daten im Internet stehen, unerlässlich und ausschlaggebend für schützende Aktionen. Dieser Aussage schließt sich die Autorin dieser Arbeit voll und ganz an. Denn erst beim Verständnis der Zusammenhänge wird ein größeres, umfangreicheres Wissen greifbar und infolge dessen umsetzbar.

Der Ansatz von Schwartz und Solove für ein neues Konzept des PII Problems ist zwar sicherlich eine Verbesserung zum Schutz von anonymisierten personenbezogenen Daten, doch im Hinblick auf Big Data zur Zeit nutzlos. Denn mit den Möglichkeiten des Data Mining bedarf es nur das aktuelle Verhalten einer Person um Rückschlüsse auf weitere

⁴⁰³ Vgl. Wu, Kuang-Wen, et al. 2012. S. 889-897

⁴⁰⁴ Vgl. Bundesamt für Sicherheit in der Informationstechnik, 26.09.2013.

persönliche Informationen schließen zu können. Es wäre unmöglich, jede einzelne Handlung zu verschlüsseln, weshalb das PII-Konzept 2.0 keine Lösung für den Schutz hinsichtlich der möglichen Big Data Folgen liefert.

13. Ausblick

Die Untersuchung zeigt auf, dass der Smartphone-Gebrauch der jungen Erwachsenen sehr ausgeprägt ist und sie täglich unzählige Daten von sich preisgeben, sei dies bewusst oder unbewusst. Das Interesse, seine eigenen Daten zu schützen ist vorhanden, allerdings mangelt es oft an der Umsetzung. Gleichzeitig besitzen viele Personen ein unzureichendes Wissen hinsichtlich Big Data und seinen Folgen. Das Bewusstsein, der Datenüberwachung während der Smartphone-Benützung ist äußerst gering und sollte zum Schutz dringend verbessert werden. Es gilt daher, den bewussten Umgang mit persönlichen Daten zu stärken, insbesondere während der Benützung, um sich so vor kritischen Folgen der Big Data-Zukunft zu schützen. Die Autorin rät, um einen ausreichenden Schutz der eigenen Daten und der Privatsphäre zu erreichen, sich über die Zugriffsrechte von Apps am eigenen Smartphone zu informieren. Dies kann durch die Beachtung der Datenschutzrichtlinien und der Zugrifferlaubnis erfolgen, wie auch durch eine Überprüfung des Datentransfers des eigenen Smartphones. Eine regelmäßige Überprüfung, insbesondere nach neuen Installationen und Updates wäre angebracht, da manche Apps Daten vom eigenen Smartphone herunterladen, ohne dies bekannt zu geben oder um Erlaubnis zu fragen.

Die Untersuchung kann als Anknüpfungspunkt für weiterführende kommunikationswissenschaftliche Studien im Bereich Big Data genutzt werden. Ziel der Studie ist es eine breite mediale Berichterstattung zu erreichen, welche dazu beitragen würde, den bewussten Umgang mit persönlichen Informationen und das Wissen bezüglich Big Data zu verbessern.

14. Limitationen der Forschung

Ressourcenbedingt umfasst die Untersuchung eine überschaubare Anzahl an persönlich geführten Leitfadeninterviews. Um ein umfassenderes und vertieftes Bild des aktuellen Wissenstandes zu erlangen, wäre eine finanziell geförderte Untersuchung notwendig um den zeitlichen Aufwand zu kompensieren.

Im Hinblick auf die Durchführung der Studie ist zu betonen, dass die leitfadengeführten Interviews sehr informativ waren und es mit Hilfe der Inhaltsanalyse schwer fiel, ein kompaktes Bild der Wissensbestände der jungen Erwachsenen zu geben. Da die Antworten im Interview zum Teil sehr unterschiedlich ausfielen, mussten die jeweiligen Kategorien weit offen gehalten werden. Es stellte sich als Herausforderung dar, die Information so knapp wie möglich, und auf das Wesentlichste reduziert, zu veröffentlichen.

15. Quellenverzeichnis

15.1. Literaturverzeichnis:

- Bentele, Günter; Brosius, Hans-Bernd; Jarren, Otfried (Hrsg.) (2013): Lexikon Kommunikations- und Medienwissenschaft. 2. Überarbeitete und erweiterte Auflage. Wiesbaden: Springer Fachmedien.
- Berger, Peter L.; Luckmann, Thomas (1966/1969): Die gesellschaftliche Konstruktion der Wirklichkeit. Eine Theorie der Wissenssoziologie. Frankfurt am Main: S. Fischer Verlag GmbH.
- Brin, David (1998): The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom? New York: Perseus Book Group.
- Burkart, Roland (2002): Kommunikationswissenschaft. Grundlagen und Problemfelder. Umriss einer interdisziplinären Sozialwissenschaft. 4., überarbeitete und aktualisierte Auflage. Wien: Böhlau Verlag.
- Deutsches Institut für Fernstudien an der Universität Tübingen (Hrsg.) (1990): Funkkolleg. Medien und Kommunikation. Konstruktionen von Wirklichkeit. Studienbrief 1. Weinheim, Basel: Beltz Verlag.
- DIVISI (02/2014): U25-Studie. Kinder, Jugendliche und junge Erwachsene in der digitalen Welt. Eine Grundlagenstudie des SINUS-Instituts Heidelberg im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVISI). Hamburg.
- Gläser, Jochen; Laudel, Grit (2009): Experteninterviews und qualitative Inhaltsanalyse als Instrument rekonstruierender Untersuchung. 3., überarbeitete Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften
- Han, Byung-Chul: Transparenzgesellschaft. 3. Auflage. Berlin: MSB Verlagsgesellschaft. 2013.
- Hasler Roumois, Ursula (2007): Studienbuch Wissensmanagement. Grundlagen der Wissensarbeit in Wirtschafts-, Non-Profit- und Public-Organisationen. Zürich: Orell Füssli Verlag Ag.
- Heller, Christian (2011): Post-Privacy. Prima leben ohne Privatsphäre. München: Verlag C.H.Beck.
- Heuer, Steffan; Tranberg, Pernille (2013): Mich kriegt ihr nicht! Gebrauchsanweisung zur digitalen Selbstverteidigung. Hamburg: Murmann Verlag.
- Hobert, Guido (2000): Datenschutz und Datensicherheit im Internet. Interdependenz und Korrelation von rechtlichen Grundlagen und technischen Möglichkeiten. 2., durchgesehene Auflage. Frankfurt am Main: Peter Lang Verlag.

- Keller, Reiner; Knoblauch, Hubert; Reichertz, Jo (Hrsg.) (2013): Kommunikativer Konstruktivismus. Theoretische und empirische Arbeiten zu einem neuen wissenssoziologischen Ansatz. Wiesbaden: Springer Fachmedien.
- Klausnitzer, Rudi (2013): Das Ende des Zufalls. Wie Big Data uns und unser Leben vorhersagbar macht. 1. Auflage. Salzburg: Ecwin Verlag.
- Knoblauch, Hubert (2014): Wissenssoziologie. 3. Auflage. Konstanz und München: UVK-Verlagsgesellschaft.
- Koidl, Roman Maria (2013): WebAttack. Der Staat als Stalker. Ein Besinnungsaufsatz. Essay. 2. Auflage. München: Wilhelm Goldmann Verlag.
- Kotteder, Franz (2011): Die wissen alles über Sie. Wie Staat und Wirtschaft Ihre Daten ausspionieren – und wie Sie sich davor schützen. 1. Auflage. München: Redline Verlag.
- Kruse, Jan (2014): Qualitative Interviewforschung. Ein integrativer Ansatz. Weinheim und Basel: Beltz Juventa.
- Kurz, Constanze; Rieger, Frank (2011): Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. Frankfurt am Main: Fischer Verlag.
- Merten; Klaus; Schmidt, Siegfried J.; Weischenberg, Siegfried (Hrsg.) (1994): Die Wirklichkeit der Medien. Eine Einführung in die Kommunikationswissenschaft. Opladen: Westdeutscher Verlag GmbH.
- Mayer-Schönberger, Viktor; Cukier, Kenneth (2013): Big Data. Die Revolution, die unser Leben verändern wird. 1. Auflage. München: Redline Verlag.
- Mayring, Philipp (2007): Qualitative Inhaltsanalyse. Grundlagen und Techniken. 9. Auflage. Weinheim: Beltz Verlag.
- Schmale, Wolfgang; Tinnefeld, Marie-Theres (2014): Privatheit im digitalen Zeitalter. Wien: Böhlau Verlag.
- Scholl, Armin (2003): Die Befragung. Sozialwissenschaftliche Methode und kommunikationswissenschaftliche Anwendung. Konstanz: UVK Verlagsgesellschaft.
- Tinnefeld, Marie-Theres; Buchner, Benedikt; Petri, Thomas (2012): Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht. 5. Auflage. München.
- Pörksen, Bernhard (2014): Konstruktivismus. Medienethische Konsequenzen einer Theorie-Perspektive. Wiesbaden: Springer Fachmedien.

Wirth, Werner (1997): Von der Information zum Wissen. Die Rolle der Rezeption für die Entstehung von Wissensunterschieden. Ein Beitrag zur Wissenskulturforschung. Opladen: Westdeutscher Verlag.

15.2. Internetverzeichnis:

Aron, Jacob (25.01.2012): New Scientist. What your online friends reveal about where you are.

Abrufbar unter: http://www.newscientist.com/article/mg21328495.500-what-your-online-friends-reveal-about-where-you-are.html#.VBcVUFck_u2 (15.09.2014)

Amtsblatt der Europäischen Gemeinschaft (12.01.2001): Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.

Abrufbar unter: <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32001R0045&from=DE> (15.09.2014)

Amtsblatt der Europäischen Gemeinschaft (31.07.2002): Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verwendung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

Abrufbar unter: <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&qid=1421060648973&from=DE> (15.09.2014)

Aulinger, Andreas; Fischer, Dirk (2000): Einige Daten und Informationen zum Wissensmanagement. DBW. Die Betriebswirtschaft, 60 (5).

Abrufbar unter: http://www.wiso-net.de/webcgi?START=A20&T_FORMAT=5&DOKM=1000436_ZECU_0&TREFFER_NR=1&WID=16152-3420944-51924_1 (22.05.2014)

Chen, Brixian X. (01.02.2013): Privacy Flaw in Path's iPhone App Shares Location Data. The New York Times. Bits. 16:11 Uhr.

Abrufbar unter: <http://bits.blogs.nytimes.com/2013/02/01/path-photos-location-loophole/> (27.06.2014)

Beuth, Partick (19.08.2011.): Die Polizei als Hellseher. In Kalifornien berechnet die Polizei voraus, wo Verbrechen geschehen werden und wartet dort auf Kriminelle. In Deutschland wäre das verfassungsrechtlich bedenklich. Zeit Online. 11:04 Uhr.

Abrufbar unter: <http://www.zeit.de/digital/datenschutz/2011-08/predictive-policing> (21.05.2014)

Bruening, Paula J. (06/ 2012): Interoperability: analysing the current trends & developments. Data Protection Law& Policy. Issue 100.

Abrufbar unter: http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/DPLP_Interoperability_Bruening.pdf (26.06.2014)

- Bundesamt für Sicherheit in der Informationstechnik (26.09.2013): Kompass zur sicheren Internetnutzung von Polizei und BSI. Stuttgart/Bonn.
Abrufbar unter: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Kompass_zur_sicheren_Internetnutzung_26092013.html (07.07.2014)
- Bundeskanzleramt Österreich: Was ist Datenschutz?
Abrufbar unter: <https://www.bka.gv.at/site/5808/default.aspx> (22.08.2014)
- Bundeskanzleramt Rechtsinformationssystem (RIS): Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Datenschutzgesetz 2000, Fassung vom 22.08.2014. DSG 2000, Art. 2 § 4 z 1,2.
Abrufbar unter: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597> (22.08.2014)
- Bundesgesetz über den Schutz personenbezogener Daten. Datenschutzgesetz 2000 – DSG 2000. Artikel 1, § 1, (1).
Abrufbar unter: <http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597> (24.04.2014)
- Chaos Computer Club e. V.: Hackerethik.
Abrufbar unter: <http://www.ccc.de/de/hackerethik> (28.05.2014)
- Datenschutz und Datensicherheit (06/2011): Datenschutzgerechte Smartphone-Nutzung ermöglichen! Datenschutz und Datensicherheit – DuD, 35 (6).
Abrufbar unter: <http://link.springer.com/article/10.1007%2Fs11623-011-0095-x> (16.05.2014)
- Deutsche Telekom AG (2014): Zahlen, Daten Fakten. Datenschutz und Datensicherheit. Bericht 2013.
Abrufbar unter: <http://telekom2.de/dud2013/> (17.05.2014)
- Dingers, Gary (13.03.2012): Lawsuit: Mobile apps accessing users' address books. Statesman. Abrufbar unter: <http://www.statesman.com/news/business/lawsuit-mobile-apps-accessing-users-address-books/nRmCT/> (27.06.2014)
- Dumbill, Edd (2012): Planning for Big Data. A CIO's Handbook to the Changing Data Landscape. Sebastopol: O'Reilly Media.
Abrufbar unter: http://cdn.oreillystatic.com/oreilly/radarreport/0636920025559/Planning_for_Big_Data.pdf (23.01.2015)
- Entscheidung der Kommission vom 26. Juli 2000. Amtsblatt der Europäischen Union. K(2000) 2441.
Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF> (29.08.2014)

EU-Initiative für mehr Sicherheit im Netz. Apps & Datenschutz.

Abrufbar unter: <http://www.klicksafe.de/themen/kommunizieren/smartphones/apps-datenschutz/> (27.08.2014)

Europäische Kommission (25.01.2012): Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundversorgung). Brüssel.

Abrufbar unter: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF> (24.04.2014)

Garante per la protezione dei dati personali: Cosa è il diritto alla protezione dei dati personali? Abrufbar unter:

<http://www.garanteprivacy.it/web/guest/home/diritti/cosa-%C3%A8-il-diritto-alla-protezione-dei-dati-personali?>* (27.08.2014)

Gerichtshof der Europäischen Union: Pressemitteilung Nr. 54/14. Luxemburg, den 8. April 2014.

Abrufbar unter: <http://malte-spitz.de/wp-content/uploads/2014/04/CP140054DE.pdf> (25.08.2014)

JIM 2014, Medienpädagogischer Forschungsverbund Südwest (11/2014): JIM 2014 Jugend, Information (Multi-) Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland. Stuttgart.

Abrufbar unter: http://www.mpfs.de/fileadmin/JIM-pdf14/JIM-Studie_2014.pdf (10.01.2015)

Kleve, Pieter; Du Mulder, Richard (2008): Privacy protection and the right to information: In search of a new balance. In: Computer Law and Security Report. 24 (3).

Abrufbar unter: <http://www.sciencedirect.com/science/article/pii/S0267364908000381> (03.07.2014)

Knapp, Moureen „Molly“ (21.11.2013): Big Data. Journal of Electronic Resources in Medical Libraries. 10 (4).

Abrufbar unter: <http://www.tandfonline.com/doi/abs/10.1080/15424065.2013.847713#.U01WDKJqzeo> (16.05.2014)

Lang, Katrin (27.06.2013): User tauschen sich gerne aus. Seven-One prüft mit Mobile Barometer Smartphone-Nutzung. Horizont 26.

Abrufbar unter: http://www.wiso-net.de/webcgi?START=A40&OVVAR=DOK_SPEICHERN,EINZEL_DOK,EINZEL_TITEL,PDF_ALLOW,RTF_ALLOW&DOK_SPEICHERN=1&EINZEL_DOK=2449691_ZECO_0&EINZEL_TITEL=SevenOne_Media_Inter&PDF_ALLOW=1&RTF_ALLOW=1&WID=67322-7360574-81226_2 (16.05.2014)

Marwick, Alice E.; Boyd, Danah (2014): Networked privacy: How teenagers negotiate context in social media. In: New Media & Society 16 (7).

- Abrufbar unter: <http://nms.sagepub.com/content/16/7/1051.full> (10.01.2015)
- McBurney, Vincent (31.05.2012): The Origin and Growth of Big Data Buss. Toolbox for IT Blog.
Abrufbar unter: <http://it.toolbox.com/blogs/infosphere/the-origin-and-growth-of-big-data-buzz-51509> (09.05.2014)
- Nemitz, Gordon; Rieder, Christian (2011): Homo Smartphone. GDI Impuls, 2.
Abrufbar unter: http://www.wiso-net.de/webcgi?START=A20&T_FORMAT=5&DOKM=1881856_ZECO_0&TREFFER_NR=1&WID=67322-7360574-81226_10 (16.05.2014)
- Perloth, Nicole (05.06.2012): LinkedIn's Leaky Mobile App Has Access to Your Meeting Notes. The New York Times. Bits. 20:00 Uhr.
Abrufbar unter: <http://bits.blogs.nytimes.com/2012/06/05/linkedins-leaky-mobile-app-has-access-to-your-meeting-notes/> (27.06.2014)
- Räth, Magdalena (14.03.2013): Dacadoo – „Gesundheit in Echtzeit“. Interview – Dacadoo will Gesundheit messbar machen und sich in diesem Sinne auch mit Krankenkassen zusammentun. Die Zürcher im Frischlings-Interview. In: Gründerszene.
Abrufbar unter: <http://www.gruenderszene.de/interviews/dacadoo> (21.05.2014)
- Rihaczek, Karl (03/2014): Transparenz. Datenschutz und Datensicherheit –DuD. 38 (3).
Abrufbar unter: http://download.springer.com/static/pdf/864/art%253A10.1007%252Fs11623-014-0063-3.pdf?auth66=1398438436_b0fe6fc9dcafe00e3ee0ce066ca93a8&ext=.pdf (24.04.2014)
- Rowinski, Dan (20.07.2012): Apple won't let you see what iPhone Apps do with your data. ReadWrite.
Abrufbar unter: <http://readwrite.com/2012/07/20/apple-wont-let-you-see-what-iphone-apps-do-with-your-data#feed=/search?keyword=apple+wont+let+you+see+what+iphone+apps+do+whit+your+data&awesm=~oInqbRkKqxRJVS> (27.06.2014)
- Schwartz, Paul M.; Solove, Daniel J. (12/2011): The PII Problem: Privacy and a New Concept of Personally Identifiable Information. In: New York University Law Review, 86 (6).
Abrufbar unter: <http://www.nyulawreview.org/sites/default/files/pdf/NYULawReview-86-6-Schwartz-Solove.pdf> (23.01.2015)
- Song, Chaoming; Qu, Zehui; Blumm, Niclas; Barabási, Albert-László (19.02.2010): Limits of Predictability in Human Mobility. Science, 327.
Abrufbar unter: http://www.barabasilab.com/pubs/CCNR-ALB_Publications/201002-19_Science-Predictability/201002-19_Science-Predictability.pdf (20.05.2014)
- Urteil des Europäischen Gerichtshofes. 08. April 2014.

Abrufbar unter:

http://curia.europa.eu/juris/document/document_print.jsf?doclang=DE&text=&pageIndex=0&part=1&mode=req&docid=150642&occ=first&dir=&cid=316886#Footnote* (25.08.2014)

Urteil des Gerichtshofes (Große Kammer) (8. April 2014).

Abrufbar unter:

<http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d2dc30d69f3cd7a602ad4afda4efdf80276db4a4.e34KaxiLc3qMb40Rch0SaxuOb3f0?text=&docid=150642&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=112813> (15.09.2014)

Wu, Kuang-Wen; Huang, Shaio Yan; Yen, David C.; Popova, Irina (2012): The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behavior. 28 (3).

Abrufbar unter:

<http://www.sciencedirect.com/science/article/pii/S0747563211002767> (03.07.2014)

Yong, Jin Park; Scott, W. Campbell; Nojin, Kwak (06/2012): Affect, cognition and reward: Predictors of privacy protection online. Computers in Human Behavior. 28 (3).

Abrufbar unter:

<http://www.sciencedirect.com/science/article/pii/S0747563212000064> (03.07.2014)

16. Anhang

16.1. Interviewleitfaden:

Institut für Publizistik- und Kommunikationswissenschaft



universität
wien

Interviewleitfaden

Vor dem Interview:

Begrüßung

Erklärung: Das Interview führen wir im Rahmen meiner Magisterarbeit an der Universität Wien zum Thema Daten und Smartphone-Nutzung.

Geht es für dich in Ordnung, wenn ich das Interview auf Tonband aufzeichne?

Deine Aussagen werden anschließend alle anonymisiert transkribiert.

Wie alt bist du, und was machst du beruflich?

Mit welchen Medien informierst du dich vorwiegend?

Täglich?

Zeitung, Zeitschriften, Radio, Internet (Social Media, Online Zeitungen), TV ...

Aufwärmphase:

Welches Smartphone besitzt du?

Für was gebrauchst du dein Smartphone?

Hast du auch Apps auf dein Smartphone heruntergeladen?

Welche dieser Apps verwendest du?

Wie oft?

Big Data:

1. Hast du schon einmal den Begriff Big Data gehört?

Wenn **Ja**:

2a. Von wem oder wo hast du davon gehört?

Kannst du mir beschreiben, was Du darunter verstehst?

Wenn **Nein**:

2b. Kannst du dir dennoch etwas darunter vorstellen?

Datenschutz:

3. Hast du den Begriff Datenschutz schon mal gehört?
4. Wie gut kennst du dich mit Datenschutz aus?
5. Erzähl mal: Was weißt du über Datenschutz?
6. Hast du den Begriff Datenschutzrichtlinie, oder Datenschutzbestimmung schon mal gehört?
7. Was steht in einer Datenschutzrichtlinie drinnen?
8. Hast du bereits einmal eine Datenschutzrichtlinie unterzeichnet?

Wenn wir nun an deine Apps denken:

9. Hast du bereits einmal eine Datenschutzrichtlinie vollständig gelesen?
10. Welche Datenschutzrichtlinien haben deine Apps?
11. Wo kann man sich über diese Datenschutzrichtlinie z.B. von Apps informieren?

Datenspeicherung:

12. Auf welche Daten von dir können Apps zugreifen?

Beispiel: Nutzt du dein Smartphone auch um Fotos zu machen?/ Du hast gesagt, du machst mit deinem Smartphone auch Fotos. Angenommen, Max benützt sein Handy immer nur zu Hause und alleine, ohne, dass sich jemand anderer neben ihm oder im gleichen Raum aufhält. Denkst du, ist es dann dennoch möglich, dass andere seine Fotos sehen können, ohne dass er sie ihnen zeigt oder schickt?

Ist es für dich realistisch, dass Max anderen erlaubt seine Fotos anzusehen, ohne dass es ihm bewusst ist? → Wieso?

13. Wie gut sind deine Fotos auf deinem Smartphone vor der Einsichtnahme anderer geschützt?
14. Wer bestimmt die Sicherheit deiner Fotos (Daten) auf deinem Smartphone?
15. Wie? Kannst du kontrollieren wer worauf zugreifen kann?

Wer, außer dir hat noch alles Zugriff auf deine Fotos, deine Kalendernotizen, dein Adressbuch usw.?

Apps?

Auf welche Bereiche haben andere (Apps) Zugriff?

16. Wie erhalten sie Zugriff?

17. Wer erlaubt ihnen das?

18. Wieso brauchen Apps Zugriff auf mehrere, verschiedene Bereiche?

Welche Daten brauchen Apps (von dir) um funktionieren zu können?

Beispiel: Könntest du dir vorstellen, dass zum Beispiel eine Wetter-App Zugriff auf das Internet braucht um zu funktionieren?

Und Zugriff auf die Kamera von deinem Smartphone aus?

Zugriff auf dein Adressbuch? Deine Fotos?

Wieso braucht sie Zugriff auf das Internet, deine Kamera, das Adressbuch und deine Fotos?

19. Was können Apps machen, wenn sie zum Beispiel den Zugriff auf deine Fotos oder dein Adressbuch haben?

Datenanalyse:

20. Was können Unternehmen machen, wenn sie unzählig viele Daten von unzählig vielen Leuten besitzen?

21. Welche Folgen kann das für uns haben?

BEISPIEL: Wenn wir annehmen, Max ladet sich eine App runter und akzeptiert bei der Installation, dass die App Zugriff auf seine Fotos, sein Adressbuch, seinen Kalender hat. Die App speichert infolge alle Informationen, also das Adressbuch, die Kalendernotizen, die Fotos, usw.

Welche Folgen könnte das für Max haben, wenn die App alle seine Daten speichert?

22. Hast du dir schon mal überlegt einen Dienst oder eine App zu löschen, weil sie zu viele Daten von dir speichern?

23. Was müsste passieren, dass du sagst, das geht jetzt eindeutig zu weit, diesen Dienst kündige ich?

24. Wie möchtest du dich in Zukunft vor Datenraub oder –Speicherung schützen?

25. Wie denkst du wird unser Leben mit dem Smartphone in 30, 50 Jahren aussehen?

Vorhersagbarkeit des Verhaltens:

Szenario 1: Wenn jemand täglich das Smartphone mit Apps und Internet zum Beispiel Twitter und/oder Facebook nützt, ohne jedoch jemals seinen Standort preiszugeben. Wäre es für dich dann vorstellbar, dass man mit großer Wahrscheinlichkeit vorhersagen kann, wo sich derjenige in Zukunft aufhalten wird?

Wieso?

Hast du schon einmal davon gehört?

Szenario 2: Wie realistisch ist es für dich, dass die Polizei bereits heute wissen kann, wo morgen ein Verbrechen stattfindet?

Wieso?

Hast du schon einmal davon gehört?

Szenario 3: Nehmen wir an, eine Frau kauft im Supermarkt verschiedene Sachen ein, jedoch keinerlei Babysachen. Kannst du dir vorstellen, dass man nur aus den gekauften Artikeln mit hoher Wahrscheinlichkeit sagen kann, ob diese Frau schwanger ist und ungefähr auch den Geburtstermin feststellen kann?

Wieso?

Hast du schon einmal davon gehört?

Folgen:

Szenario 4: Nehmen wir an, ein Mann ist homosexuell, er nützt das Internet, darunter auch Social Media, gibt jedoch nirgends an, dass er Männer liebt. Sein Sexualleben wird also von ihm nicht preisgegeben - weder im Internet, noch sonst irgendwo. Für wie realistisch hältst du es, dass wildfremde Personen dennoch mit hoher Wahrscheinlichkeit sagen können, dass der Mann homosexuell ist?

Wieso?

Hast du schon einmal davon gehört?

Szenario 5: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft deine Freundesliste auf Facebook kontrollieren und auch die Bewegungsdaten von deinem Smartphone heranziehen, wenn sie prüfen wollen, ob du kreditwürdig bist oder nicht?

Wieso?

Hast du schon einmal davon gehört?

Szenario 6: Kennst du die Gesundheits- und Fitness-Apps die man am Smartphone herunterladen kann?

Kannst du dir vorstellen, dass in Zukunft Gesundheitsversicherungen prüfen, ob du regelmäßig Sport machst und ob du dich gesund ernährst, wenn du eine Versicherung bekommst?

Wieso?

Hast du schon einmal davon gehört?

Szenario 7: Wie wahrscheinlich hältst du das Szenario, dass man in Zukunft in ein Land nicht mehr einreisen darf, weil man zum Beispiel ein bestimmtes Wort im Internet eingegeben hat?

Wieso?

Hast du schon einmal davon gehört?

Szenario 8: Ist es für dich realistisch, dass man aus dem Verhalten der Vergangenheit, das Verhalten in der Zukunft schon vorhersagen kann?

Danke für das Interview.

16.2. Transkriptionsregeln:

[abc]	Einfügung von der Autorin
[...]	Auslassung von der Autorin
(?)	Unverständlicher Wortlaut
(abc?)	Vermuteter Wortlaut
[Pause]	längere Pause
A: Abc Abc Abc, ...	Sprechende Person wird unterbrochen
I: ..., edf, edf, edf.	

16.3. Transkribierte Interviews

Die Interviews werden nach der Reihe der Durchführung aufgelistet.

1 **Interview 1 am 19.09.2014. Dauer 21:45 Minuten**

2

3 A: Wie alt bist du und was machst du beruflich?

4 I: Ich bin 21 und ich bin Beruf 1.

5 A: Was ist deine höchste abgeschlossene Ausbildung.

6 I: Die Matura.

7 A: Mit welchen Medien informierst du dich vorwiegend?

8 I: Über was?

9 A: Generell.

10 I: Ja, übers Internet meistens, übers Handy. Zeitung auch ein bisschen, aber mehr übers
11 Handy.

12 A: Und was machst du im Internet?

13 I: Ja Ding lesen, so, wie sagt man, weißt du N24, NTv, so Nachrichtensender, von denen die
14 Artikel lesen und solche Sachen.

15 A: Ok, machst du das täglich?

16 I: Ja.

17 A: Welches Smartphone besitzt du?

18 I: Marke 4 Model 4.

19 A: Wofür gebrauchst du dein Smartphone?

20 I: Ja für was? Ja für Telefonieren, SMS, WhatsApp, Internet, normal. Ein bisschen Musik,
21 aber das nicht so häufig.

22 A: Wecker? Kalender?

23 I: Ja, Wecker ja, Kalender weniger.

24 A: Fotos?

25 I: Ein bisschen.

26 A: Also machst du wenige Fotos mit deinem Handy?

27 I: Ja, nicht so viele. Nur spontane Fotos.

28 A: Hast du dir auch Apps auf dein Smartphone heruntergeladen?

29 I: Ja, das hab ich auch heruntergeladen.

30 A: Welche?

31 I: Ja die normalen halt, WhatsApp und das alles und dann so Programme, mit denen man
32 Lieder speichern kann und Videos und so, so wie YouTube, wenn man es anschaut hat man es
33 auf dem Handy. Und dann noch, ja was hab ich noch für welche Apps? Ja ein paar Spiele.
34 Und Google Maps und so und dann hab ich noch für so Flugsuche und so was.

35 A: Facebook auch?

36 I: Jaja, Facebook, sowieso.

37 A: Taschenlampe oder Wetter App?

38 I: Ja, das auch, beides.

39 A: Wie oft nutzt du diese?

40 I: Die Apps?

41 A: Ja.

42 I: Ja, wenn du sagst Facebook immer eigentlich. Wie oft am Tag meinst du?

43 A: Nein, täglich oder wie oft nützt du die anderen?

44 I: Ja die anderen wenn ich sie brauche, sporadisch. Die Spiele öfter, aber das andere, wenn ich

45 es gerade brauch.

46 A: Die Spiele jeden Tag oder fast jeden Tag?

47 I: Ja, mehrmals pro Tag.

48 A: Hast du schon einmal den Begriff Big Data gehört?

49 I: Nein.

50 A: Könntest du dir dennoch vorstellen, was damit gemeint ist?

51 I: Big Data... ja viele Daten, nein keine Ahnung, ich weiß es nicht.

52 A: Hast du den Begriff Datenschutz schon mal gehört?

53 I: Ja.

54 A: Wie gut kennst du dich mit Datenschutz aus?

55 I: Ah, nicht so gut.

56 A: Erzähl mal, was weißt du über Datenschutz?

57 I: Ja, dass welche Dateien, welche Informationen über dich im Internet gespeichert werden

58 und was auch aufscheint zum Beispiel, wenn du, was die anderen über dich herausfinden

59 können im Internet oder was alles drinnen ist von dir. Ja und was die Firmen, so Suchverläufe

60 und so, was die alles speichern und was in anderen auch angezeigt wird und so halt.

61 A: Ist das nur auf das Internet bezogen?

62 I: Nein, sonst schon auch, bei allem. Überall wo du deine Daten und deine Sachen angeben

63 musst.

64 A: Ok. Heißt das, dass deine Daten jeder sehen kann?

65 I: Kommt drauf an, wie du es eingestellt hast.

66 A: Wie du sie schützt?

67 I: Ja genau.

68 A: Datenschutzbestimmung oder Datenschutzrichtlinie, hast du davon schon mal gehört?

69 I: Ja, aber noch nie durchgelesen. Das ist immer so ein (fetter Fleck?).
70 A: Was steht denn in einer Datenschutzrichtlinie drinnen?
71 I: Das weiß ich nicht.
72 A: Hast du noch nie eine angesehen?
73 I: Nein.
74 A: Hast du schon einmal eine Datenschutzrichtlinie unterzeichnet, also unterschrieben?
75 I: Ja, keine Ahnung, bei der Bank ist das sicher.
76 A: Nur bei der Bank oder sonst noch irgendwo?
77 I: Keine Ahnung, ja kann sicher sein. Jetzt fällt mir aber gerade nichts ein.
78 A: Weißt du jetzt aber keine?
79 I: Nein.
80 A: Wenn du jetzt an deine Apps denkst, meinst du, dass deine Apps eigene
81 Datenschutzrichtlinien haben?
82 I: Ja.
83 A: Hast du dir eine Datenschutzrichtlinie von einer App bereits einmal vollständig
84 durchgelesen?
85 I: Nein.
86 A: Welche Datenschutzrichtlinien haben denn deine Apps?
87 I: Wenn ich sie nie gelesen hab, wie soll ich das dann wissen?
88 A: Ungefähr hast du eine Ahnung was drinnen stehen könnte?
89 I: Ja keine Ahnung, was halt gespeichert wird, über die Sachen die ich im Internet tue. Wann
90 ich drinnen bin, was ich mache, wem ich schreibe oder ... Wie viel gespeichert wird von
91 diesen Sachen.
92 A: Aber nur wenn du mit den Apps in das Internet gehst oder sonst auch?
93 I: Nein, nein, schon sonst auch. Standorte und so werden ja auch oft ...
94 A: Wo kann man sich über die Datenschutzrichtlinien von den Apps zum Beispiel jetzt genau
95 informieren?
96 I: Keine Ahnung, wenn es dich interessiert, kannst du sicher ... ja etwas steht ja immer dabei
97 bei der App, sobald man sie herunterladet, Datenschutz und so. Oder sonst kannst du es sicher
98 googeln oder es gibt sicher so Foren, für solche Leute wie dich, die genau schreiben, was das
99 [die App] alles macht und so.
100 A: Aber das hast du gesehen, dass wenn man die App herunterladet, ...
101 I: ... ja das tut man ja immer akzeptieren, aber das liest ja niemand.
102 A: Ok, also unterschreibst du praktisch?

103 I: Ah, ok, unterschreiben, digital.

104 A: Auf welche Daten können denn deine Apps zugreifen?

105 I: Keine Ahnung, auf ... ja wahrscheinlich wo ich bin, ja gerade mit wem ich schreibe, mit

106 wem ich telefoniere vielleicht. Dann wie oft ich das Handy ...

107 A: ... Konkret die Nachtrichten meinst du jetzt, dass man direkt die Nachrichten lesen kann,

108 oder nur wissen, ok du ...

109 I: ... nein, mehr nur, dass ich um 12 Uhr der Person 1 geschrieben habe oder so, oder dieser

110 Nummer geschrieben habe. Vielleicht Nachrichten nicht unbedingt lesen, obwohl das können

111 sie sicherlich auch irgendwie, aber nein, das interessiert ja niemanden.

112 A: Ok, vor allem Standort und?

113 I: Ja und was hab ich noch gesagt? Was ich schreibe und was ich tue und wann ich online bin

114 und was noch vielleicht? Ja so mein Ding so. So von mir ein Profil zu erstellen. Zum Beispiel,

115 wenn ich etwas suche auf Google, für Werbungen und solche Sachen, dass sie mir dann,

116 genau für mich die Werbung zeigen, wo sie denken, dass könnte ich kaufen und solche

117 Sachen.

118 A: Du nützt dein Handy ja auch um Fotos zu machen, hast du gesagt.

119 Ich schildere dir jetzt ein Szenario: Angenommen der Max nützt sein Handy immer nur zu

120 Hause, alleine und ohne, dass dich jemand anderer im gleichen Raum oder neben ihm

121 aufhält, denkst du ist es dann dennoch möglich, dass andere seine Fotos sehen können, auch

122 wenn er ihnen diese weder zeigt, noch schickt?

123 I: Wenn er sie online stellt meinst du?

124 A: Nein, nicht online, einfach nur auf seinem Handy hat er die Fotos.

125 I: Wenn sie jemand will, jaja, wenn sie das irgendwie hacken oder so, irgendwie geht das

126 sicher. Über WLAN sowieso, über öffentliches WLAN.

127 A: Könntest du dir vorstellen, dass er ihnen das sogar erlaubt anzusehen, aber es ihm nur nicht

128 bewusst ist?

129 I: Ja erlaubt kann schon sein, aber bewusst wird es nicht sein. Das wird er halt irgendwo

130 akzeptiert haben, aber dass sie es sogar ansehen können? Kann schon sein. Jaja, das kann ich

131 mir schon vorstellen.

132 A: Wie gut sind denn deine Fotos auf deinem Smartphone vor der Einsichtnahme anderer

133 Personen geschützt?

134 I: Überhaupt nicht.

135 A: Hast du nichts vorgenommen, oder so?

136 I: Wie, dass man ein Passwort oder so eingeben muss?

137 A: Ja das ,oder wie wir gesagt haben mit den Apps, dass diese zugreifen können?
138 I: Ah nein.
139 A: Hast du nie kontrolliert?
140 I: Nein.
141 A: Kannst du kontrollieren worauf andere Leute zugreifen können, auch Dienstleistungen,
142 wie Apps und das Internet und so?
143 I: Ja das zeigt es dir wohl an, wenn du es herunterlädst, dass das auf Standort, und das worauf
144 es zugreift.
145 A: Hast du das schon mal kontrolliert?
146 I: Nein, ich schau es mir halt an.
147 A: Wer außer dir hat noch alles Zugriff auf deine Fotos, deinen Kalender, dein Adressbuch,
148 deinen Standort?
149 I: Ja eigentlich niemand, normal. Sicher jeder, aber bewusst niemand. Ich kann mir vorstellen,
150 dass irgendjemand, irgendwie das jeder herausfinden könnte, wenn man ein bisschen
151 fanatisch ist.
152 A: Aber, dass du es ihnen erlaubt hast?
153 I: Bewusst? Nein, das eigentlich nicht. Außer es ist so eine App, wo das dabei ist, und ich das
154 nicht gelesen habe.
155 A: Wo du das dann einfach akzeptiert hast?
156 I: Jaja, genau.
157 A: Jetzt haben wir das eigentlich schon besprochen. Wie bekommen denn die Apps Zugriff
158 auf deine Bereiche?
159 I: Ja wenn ich sie herunterlade und die dann akzeptiere, dann können sie tun was sie wollen.
160 A: Dann erlaubst du ihnen den Zugriff sozusagen?
161 I: Ja genau.
162 A: Wieso meinst du brauchen die Apps Zugriff auf verschiedene Bereiche auf deinem Handy?
163 I: Einmal sicher um zu funktionieren, und dann sicher auch, damit sie sich finanzieren
164 können, zum Beispiel mit der Werbung und solchen Sachen. Und oft auch zum Beispiel um
165 Daten zu stehlen, das weiß man oft nicht, wenn man mindere Apps herunterladet, dann
166 werden diese das [die Daten] irgendwo speichern und verkaufen. Keine Ahnung.
167 A: Was machen die Apps, wenn sie deine Daten speichern?
168 I: Wie, was machen sie?
169 A: Du hast ja gesagt, für Werbung. Aber wieso verkaufen sie deine Daten an andere
170 Unternehmen?

171 I: Ja für Geld, damit sie Geld bekommen.

172 A: Was machen dann die anderen Unternehmen mit deinen Daten?

173 I: Werbungen und solche Sachen, denk ich mir.

174 A: Was meinst du können Unternehmen machen, wenn sie unzählig viele Daten von dir

175 haben? Und nicht nur von dir, sondern von unzählig vielen andern Leuten. Gibt es noch einen

176 anderen Gedanken außer Werbung?

177 I: Sicher, wenn sie Passwörter von Internetseiten oder Kreditkarten haben. Aber das mache

178 ich nicht über das Handy. Vielleicht erpressen sie dich auch. Aber das glaube ich nicht. Was

179 sie sonst noch machen könnten mit diesen Daten? Ich wüsste es nicht.

180 A: Hast du dir schon mal überlegt einen Dienst oder eine App zu löschen, weil sie zu viele

181 Daten von dir speichern?

182 I: Nein. Ich denke mir, das, was ich auf meinem Smartphone habe, das ist für mich nicht

183 schlimm, wenn sie das sehen.

184 A: Was müsste passieren, dass du sagst das geht jetzt eindeutig zu weit, diesen Dienst

185 kündige ich?

186 I: Hm, ja wenn ich auf einmal private Sachen von mir im Internet öffentlich sehe oder so.

187 Oder ich wegen diesen Daten von einem Amt oder so, etwas nicht bekommen würde.

188 A: Wie möchtest du dich in Zukunft vor Datenraub oder –Speicherung schützen?

189 I: Ja, im Grunde darauf achten, was die Apps von mir haben wollen. Nicht zu viele Daten

190 preisgeben.

191 A: Wie denkst du wird unser Leben mit dem Smartphone in 30, 50 Jahren aussehen?

192 I: Dann wird man alles über das Handy machen, von bezahlen über Essen bestellen, ja alles.

193 A: Müssen wir dann überhaupt noch was machen oder macht das Handy alles alleine?

194 I: Wie machen?

195 A: Entwickelt sich das dann weiter, dass wir nicht mehr einkaufen gehen müssen?

196 I: Ja sicher. Irgendwann wird man nur mehr eingeben was man will und dann steht es am

197 Abend vor der Haustür.

198 A: Meinst du, dass wir überhaupt noch eingeben müssen was wir brauchen?

199 I: Nein, das auch nicht mehr. Oft wird es schon Vorschläge machen, denk ich mir, wenn es

200 sieht: ah der [dieser Mensch] hat das gekauft, dann könnte er das auch kaufen. Das ist ja bei

201 Amazon auch schon. [...]

202 A: Jetzt beschreibe ich dir ein paar Szenarien und frage dich, ob diese für dich realistisch sind

203 oder nicht und warum.

204 Könntest du dir vorstellen, dass wenn jemand täglich sein Smartphone mit Apps und Internet,

205 zum Beispiel Twitter und/oder Facebook, nützt, ohne dass er jemals seinen Standort preisgibt.
206 Wäre es für dich dann vorstellbar, dass man mit großer Wahrscheinlichkeit vorhersagen kann,
207 wo sich derjenige in Zukunft aufhalten wird?
208 I: Hm. Sie wissen nie wo du gewesen bist?
209 A: Nein, der Standort wird nicht freigegeben.
210 I: Sie können aber auch über das Handysignal schon wissen wo du ungefähr bist.
211 A: Auch das wird nicht berücksichtigt.
212 I: Dann müssten sie es herausfinden nur über das was man schreibt und postet?
213 A: Zum Beispiel.
214 I: Dann können sie in Zukunft sagen wo du sein wirst? Ja, keine Ahnung. Kann schon sein.
215 Könnte ich mir schon vorstellen.
216 A: Weißt du davon oder wieso kannst du dir das vorstellen?
217 I: Weil die einfach unglaublich fanatisch sind. Und das wird ihnen schon irgendwie nutzen,
218 dass sie Geld verdienen, wenn sie sehen wo jemand ist. Keine Ahnung. Irgendwie, wenn sie
219 rausfinden wo du immer warst, dann wissen sie ja auch was dir gefällt und könnten sie dir
220 zum Beispiel, ... aber sie sagen dir ja nicht wohin du gehen sollst... aber sie könnten dir
221 sagen, das könnte dir auch gefallen, oder da musst du auch hin, aber dass sie wissen, dass du
222 alleine dort hin gehst und sie wissen, dass du dort bist... Vielleicht machen sie ein Profil von
223 dir, und dann sagen können, was du immer machst.
224 A: Wenn sie aber keine Standortangaben über dich haben, denkst du, kann man dann dennoch
225 mit hoher Wahrscheinlichkeit sagen, dass sich jemand mit großer Wahrscheinlichkeit morgen
226 an einem gewissen Punkt befindet?
227 I: Ich würde eher sagen nicht. Ich bin mir unsicher.
228 A: Hast du davon schon mal was gehört?
229 I: Nein.
230 A: Nächstes Beispiel: Wie realistisch ist es für dich, dass die Polizei bereits heute wissen
231 kann, wo morgen ein Verbrechen stattfindet?
232 I: Wenn jemand nichts mit dem Handy macht?
233 A: Nein, nichts.
234 I: Das ist unrealistisch. Wenn ich mir denke ich gehe dort morgen hin und raube diese Bank
235 aus, dann können sie das nicht wissen. Würde ich sagen. Außer ich schriebe das auf
236 Facebook.
237 A: Nein, das ist eine andere Sache. Kannst du dir zum Beispiel vorstellen, dass die Polizei aus
238 früheren Verbrechen ein Muster erstellen kann, wo in Zukunft nach Verbrechen stattfinden können?

239 I: Aso, hm. Ja das ist schon möglich, wenn sie die Verbrechen von früher analysiert, aber,
240 dass sie dann weiß wo morgen eines stattfinden kann, halte ich für unrealistisch.

241 A: Nehmen wir an, eine Frau kauft im Supermarkt verschiedene Sachen ein, jedoch keinerlei
242 Babysachen. Kannst du dir vorstellen, dass man nur aus den gekauften Artikeln mit hoher
243 Wahrscheinlichkeit sagen kann, ob diese Frau schwanger ist oder nicht ...

244 I: ... und das Baby ist schon auf der Welt?

245 A: Nein, das Baby ist noch nicht auf der Welt. Sie ist nur schwanger oder auch nicht. Kannst
246 du dir vorstellen, dass man dann sagen kann, ob die Frau schwanger ist und ungefähr auch
247 sagen wann der Geburtstermin ist?

248 I: Nein, ich sag nicht.

249 A: Wieso nicht?

250 I: Keine Ahnung.

251 A: Nehmen wir an, ein Mann ist homosexuell, er nützt das Internet, darunter auch Social
252 Media, gibt jedoch nirgends an, dass er Männer liebt. Er gibt sein Sexualleben nirgends preis
253 – sieht sich auch nichts an, was in diese Richtung deuten könnte, ...

254 I: ...bei Google sucht er auch nie?...

255 A: ... nein, bei Google sucht er auch nie. Für wie realistisch hältst du es, dass wildfremde
256 Personen dennoch mit hoher Wahrscheinlichkeit sagen können, dass der Mann homosexuell
257 ist?

258 I: Ich denk schon.

259 A: Wieso?

260 I: Er wird schon andere Sachen suchen, nicht unbedingt: Wo kann ich homosexuelle Männer
261 treffen, aber vielleicht von den Sachen die sie zum Beispiel bei Amazon kaufen oder
262 überhaupt wird man das schon sagen können. Ich denk schon.

263 A: Und wie funktioniert das, wenn es zum Beispiel so ist, dass homosexuelle Männer
264 vorwiegend gelbe T-Shirts tragen. Wie funktioniert das dann, wenn er ein gelbes T-Shirt
265 kauft, dass er dann als homosexuell eingestuft wird?

266 I: Weil sie davon ausgehen, vielleicht. Es muss ja nicht unbedingt so sein, vielleicht gefällt es
267 ihm nur so, und sucht dann zufällig das gleiche oder tut zufällig das gleiche wie ein
268 Homosexueller. Und weil sie das dann so deuten, fällt er in diese Sparte hinein. Es wird dann
269 gesagt: alle die das so machen... Da gibt es dann keine Ausnahmen, für die ist dann alles das
270 Gleiche.

271 A: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft deine Freundesliste auf Facebook
272 kontrollieren und auch die Bewegungsdaten von deinem Smartphone heranziehen, wenn sie
273 prüfen wollen, ob du kreditwürdig bist oder nicht?

274 I: Ja.

275 A: Wieso?

276 I: Ich denk schon. Damit sie sehen, was das für ein Mensch ist, dem sie das Geld geben.

277 A: Hast du schon einmal davon gehört?

278 I: Nein, aber zum Beispiel [Person erzählt Ereignis aus ihrem eigenen Leben, das dieses
279 Beispiel genau erklärt.]

280 A: Hast du das von anderen Personen gehört oder gelesen?

281 I: Ja, von Person 2.

282 A: Kennst du die Gesundheits- und Fitnessapp's, wo man eingibt was man isst oder wie viel
283 man trainiert?

284 I: Jaja, kenn ich schon.

285 A: Kannst du dir vorstellen, dass in Zukunft Gesundheitsversicherungen prüfen, ob du
286 regelmäßig Sport machst und wie du dich ernährst, wenn sie schauen, ob du eine
287 Versicherung bekommst oder nicht? Eine Gesundheitsversicherung?

288 I: Ja, das kann schon sein.

289 A: Wieso?

290 I: Da werden sie auch wieder so verschiedene Klassen haben. Damit sie sagen zu diesem Preis
291 können wir es dieser Person anbieten, weil sie macht jeden Tag Sport, isst gesund und dann
292 ist die Wahrscheinlichkeit weniger hoch, dass sie [die Versicherungsgesellschaft] zahlen
293 muss. Dafür kann sie es [die Versicherung] billiger machen, oder auch im Fall nicht
294 versichern, wenn sie denken, der könnte eventuell teuer werden.

295 A: Für wie wahrscheinlich hältst du das Szenario, dass man in Zukunft in ein Land nicht mehr
296 einreisen darf, weil man zum Beispiel ein bestimmtes Wort, entweder in einer SMS
297 geschrieben hat, in Facebook, oder im Internet eingegeben hat?

298 I: Ja, das gibt es sicher. Das gibt es in Amerika sicher auch schon.

299 A: Hast du schon einmal davon gehört?

300 I: Nein, jetzt genau nicht. Aber das kann ich mir leicht vorstellen. Das gibt es sicher jetzt
301 schon, dass wenn du einmal Bombe, oder Bombe selber bauen, gesucht hast, dann lassen sie
302 dich nicht mehr einreisen. Das glaub ich gleich. Bei den Amerikanern sicher.

303 A: Ist es für dich realistisch, dass man aus dem Verhalten der Vergangenheit, das Verhalten in
304 der Zukunft schon vorhersagen kann?

305 I: Sicher nicht für jeden einzelnen, aber für die große Masse, dass sie das ungefähr sagen
306 können, normalerweise müsste der... Ja sicher. Bei jedem wird es nicht zutreffen, aber bei
307 vielen Leuten sicher.

308 A: Also nicht mit hoher Wahrscheinlichkeit?

309 I: Doch, doch das schon. Über 50 Prozent. Es gibt sicher auch Fälle, wo es sich anders
310 entwickelt, aber eher wahrscheinlich als unwahrscheinlich.

311 A: Du hast gesagt nicht für jeden. Also nur für bestimmte oder für wen gilt das dann?

312 I: Das kann man so nicht sagen. Sie können sagen normalerweise, wenn er sich so und so
313 verhält, dann wird das so und so. Wenn sie Erfahrungen und Werte von früher haben. Es
314 muss aber nur bei jemanden mal was passieren, oder anders werden, dass das dann komplett
315 nicht mehr zutrifft.

316 A: Nehmen wir mal an, jemand gibt sehr wenige Daten ins Internet ein, können sie dann
317 dennoch das Verhalten vorhersagen, oder dann weniger?

318 I: Doch, das ist für sie ja auch wieder ein Hinweis. Wenn jemand nichts preisgibt, sind das ja
319 wiederum Daten, die in eine Richtung deuten. Könnte ich mir denken.

320 A: Also hängt es im Grunde nicht davon ab, wie viel jemand preisgibt, sondern von dem wie
321 es ausgerechnet wird?

322 I: Ja, genau. Was dann nicht unbedingt stimmen muss, aber ich kann es mir vorstellen, denn
323 sie verdienen ja Geld damit, deswegen müssen sie es ja gut machen. Sonst wäre es ja umsonst.

324 A: Danke für das Interview.

- 1 **Interview 2, am 19.09.2014. Dauer 17:13 Minuten**
- 2 A: Wie alt bist du und was machst du beruflich?
- 3 I: Ich bin 20 Jahre alt und Beruf 3.
- 4 A: Was ist deine höchste abgeschlossene Ausbildung?
- 5 I: Die Matura.
- 6 A: Mit welchen Medien informierst du dich vorwiegend?
- 7 I: Meistens im Internet und Fernsehen ein bisschen, aber Zeitung ganz selten.
- 8 A: Und im Internet so Seiten, oder auch auf Facebook Benachrichtigungen von Stol oder so?
- 9 I: Ja das ist es meistens, genau.
- 10 A: Ok, ist das täglich?
- 11 I: Ja.
- 12 A: Welches Smartphone besitzt du?
- 13 I: Wie es heißt? Marke 5.
- 14 A: Ja, das kenne ich. Für was gebrauchst du es?
- 15 I: Meistens zum Schreiben, dann Facebook so ein bisschen lesen und für Thema 1, die
- 16 Ergebnisse zu schauen. Das war's.
- 17 A: Internet also? Telefonieren? Apps? Fotos?
- 18 I: Ja. Ja, das auch alles.
- 19 A: Wie sieht es aus mit Wecker und Kalender?
- 20 Wecker ja, Kalender nutze ich nicht so.
- 21 A: Hast du dir auch Apps heruntergeladen?
- 22 I: Ja.
- 23 A: Welche?
- 24 I: WhatsApp, dann ein paar Spiele, ...
- 25 A: ... ja...
- 26 I: ... aber die sind von einem Kolleg und Thema1 App, da kann man beim Thema 1 die
- 27 Liveergebnisse ansehen.
- 28 A: Facebook?
- 29 I: Ja, das auch.
- 30 A: So Taschenlampe, Wetter?
- 31 I: Ja genau.
- 32 A: Wie oft nutzt du diese Apps?
- 33 I: Täglich eigentlich, ja.
- 34 A: Alle mehr oder weniger?

35 I: Mehr oder weniger schon, ja.

36 A: Ok. Hast du schon mal vom Begriff Big Data gehört?

37 I: Nein.

38 A: Könntest du dir aber dennoch vorstellen, was das sein könnte?

39 I: Nein, keine Ahnung.

40 A: Datenschutz ist dir das ein Begriff?

41 I: Ja.

42 A: Wie gut kennst du dich mit Datenschutz aus?

43 I: Ganz schlecht. Weil ich zum Beispiel tue auch so wenig wie möglich hinein [ins Internet

44 stellen], dann denke ich mir wird das schon passen, aber da kenn ich mich nicht gut aus.

45 A: Wenn du jetzt jemanden erzählen müsstest was Datenschutz ist, was würdest du dann

46 sagen?

47 I: [Pause] Das ist da, um deine Daten vor öffentlichen Sachen zu schützen.

48 A: Nur öffentlich oder sonst auch irgendwie?

49 I: Ja, dass sie nicht für jedermann zugänglich sind.

50 A: Datenschutzrichtlinie, hast du das schon mal gehört?

51 I: Nein.

52 A: Datenschutzbestimmung, oder so was?

53 I: Nein, gar nichts.

54 A: Dann wirst du auch nicht wissen, was drinnen steht in so einer Datenschutzrichtlinie, oder?

55 Nein.

56 A: Glaubst du, hast du schon mal eine unterzeichnet?

57 I: Ich glaube das kann sein. Wenn du dich heute bei Facebook und so anmeldest und wo du

58 anklicken musst, was keiner durchliest, damit es immer weiter geht.

59 A: Zu akzeptieren, das?

60 I: Ja.

61 A: Meinst du haben deine Apps auch Datenschutzrichtlinien?

62 I: [Pause] Ja, ich denke schon. Mir kommt schon vor.

63 A: Hast du irgendwann mal eine gelesen von diesen Datenschutzrichtlinien?

64 I: Nein, nie.

65 A: Was meinst du welche Richtlinien beim Datenschutz deine Apps haben?

66 I: Was da drinnen steht?

67 A: Ja, was sie schützen müssen.

68 Ich denke mir mal, dass nicht andere Sachen von meinen Handy da rein (ins Internet)
69 kommen.

70 A: Wie meinst du andere Sachen?

71 I: Wenn du Fotos machst, dass Facebook dann nicht das von deinem Handy herunterladen
72 kann oder ansehen kann. Solche Sachen denke ich mir, hauptsächlich.

73 A: Dass praktisch diese Seiten keinen Zugriff haben.

74 I: Ja genau.

75 A: Wo meinst du kann man sich informieren über diese Richtlinien von den Apps.

76 I: Bei der App selbst, wenn man sie öffnet, dann kommt mir vor, hab ich das mal gesehen.
77 Und sonst am Anfang, wenn du sie herunterladest, wenn du es dir durchliest.

78 A: Was musst du da tun?

79 I: Durchlesen kann man es und akzeptieren.

80 A: Ok, dass man sie überhaupt nutzen kann.

81 I: Ja.

82 A: Was meinst du: Auf welche Daten können deine Apps zugreifen? Können sie überhaupt
83 auf Daten zugreifen, und wenn ja auf welche?

84 I: Ich hoffe auf keine. Aber wenn, dann denke ich zum Beispiel Facebook vor allem, was man
85 liked und so. Denk ich mir. Oder Kommentare oder wenn du was erwähnst oder so.

86 A: Du nutzt dein Smartphone auch, um Fotos zu machen, oder?

87 I: Ja.

88 A: Angenommen der Max nutzt sein Handy immer nur zu Hause, alleine und ohne, dass sich
89 jemand anderer im gleichen Raum oder neben ihm aufhält, denkst du ist es dann dennoch
90 möglich, dass andere seine Fotos sehen können, auch wenn er ihnen diese weder zeigt, noch
91 schickt?

92 I: Ja, wenn er Internet hat auf dem Handy sicher.

93 A: Wieso?

94 I: Ja, dann kannst du dir das herunterladen. Es gibt ja auch solche Programme wo man auf das
95 Handy von anderen zugreifen kann, dann siehst du auf deinem Bildschirm das, was auch der
96 andere sieht.

97 A: Aber wie bekommen die App Zugriff? Ist das dann illegal?

98 I: Ja das wohl, aber wie sie das machen weiß ich selbst nicht.

99 A: Könntest du dir aber vorstellen, dass der Max erlaubt, anderen Leuten seine Fotos
100 anzusehen, ohne dass es ihm bewusst ist?

101 I: Das könnte sein, ja. Ja, wenn er etwas bestätigt oder so, das könnte schon sein.

102 A: Was wäre etwas bestätigen?
103 I: Nutzungsbedingungen oder so.
104 A: Wie gut meinst du sind deine Fotos vor der Einsicht anderer Personen geschützt?
105 I: Ich hoffe gut, aber (lacht). Ja aber ich denke schon gut, weil so viel lade ich nicht herunter
106 und ich bin eigentlich immer auf den selben Seiten, deswegen müsste das schon passen.
107 A: Aber die Nutzungsbedingungen hast du dir noch nie durchgelesen?
108 I: Nein.
109 A: Wer bestimmt die Sicherheit deiner Fotos? Wer kann da sagen, wie gut diese geschützt
110 sind?
111 I: Ja vor allem wir selbst denk ich mir, wenn wir uns das durchlesen. Aber sonst wüsste ich
112 das nicht.
113 A: Kannst du das auch kontrollieren, wer auf was Zugriff hat?
114 I: Nein, das sehe ich nicht.
115 A: Wer meinst du, hat außer dir noch Zugriff auf deine Fotos, deinen Kalender, dein
116 Adressbuch?
117 I: Ja ich, ich hoffe sonst keiner. Und sonst große Firmen, die die Daten brauchen und
118 weiterverkaufen und so was.
119 A: Das wären dann zum Beispiel Apps?
120 I: Ja, so was.
121 A: Auf welche Bereiche meinst du haben die dann genau Zugriff?
122 I: Vor allem auf die wo es um Wirtschaft geht, was man liked und so. Auf Telefonnummern
123 und so denke ich weniger, Fotos und solche Sachen.
124 A: Und wie erhalten die überhaupt Zugriff?
125 I: Durch die Apps vielleicht, wenn man etwas herunterladet, oder wenn sie dich hacken oder
126 du auf einer Seite etwas anklickst.
127 A: Wenn du ihnen das erlaubst?
128 I: Ja genau.
129 A: Wieso brauchen Apps zum Beispiel Zugriff auf mehrere Bereiche?
130 I: Damit die mehr Leute erreichen können und mehr verdienen, so mehr für Werbung
131 bekommen und so, denke ich mir.
132 A: Wenn du jetzt an eine App denkst. Welche Daten braucht sie von dir, damit sie überhaupt
133 funktionieren kann?
134 I: Telefonnummer, den Namen muss man manchmal eingeben, und die E-Mailadresse immer.
135 Ja diese Daten vor allem.

136 A: Du hast ja gesagt, dass diese Unternehmen die Daten weiterverkaufen. Was können denn
137 Apps machen, wenn sie Zugriff auf deine Fotos, dein Adressbuch u.s. w. haben. Was nutzt
138 ihnen das?

139 I: Damit sie die Werbung auf jemanden genau zuschneiden können. Dass sie genau wissen,
140 zum Beispiel mir gefällt Thema 1, weil ich alles bei Thema 1 like, dass sie dann genau
141 wissen, wie sie die Werbung zuschneiden müssen.

142 A: Kannst du dir noch was vorstellen, außer Werbung?

143 I: Weiterverkaufen, aber was dann genau...

144 A: Was machen Firmen zum Beispiel, die Daten kaufen?

145 I: Die kaufen Daten und verkaufen diese dann natürlich auch weiter, damit sie die Werbung
146 optimieren können und sie genau auf die Leute zuschneiden können.

147 A: Und diese Firmen, die interessiert sind an diesen Daten, was machen diese dann damit?

148 I: Weiterverwenden um zu kontrollieren, was sie verbessern können an ihren Produkten und
149 so.

150 A: Welchen Nutzen, außer Werbung, können Unternehmen noch auch Daten ziehen?

151 I: Das wüsste ich jetzt nicht.

152 A: Wenn du dir vorstellst ein Unternehmen hat unzählig viele Daten von vielen Leuten. Was
153 können diese dann damit tun?

154 I: Ja, zum einen weiterverkaufen an andere Firmen, zum anderen, wenn sie selbst Produkte
155 haben, für sich selbst nutzen. Ja, in diesem Bereich denk ich mir.

156 A: Welche Folgen hat das dann für uns?

157 I: Dass wir weniger Privatsphäre haben (...?).

158 A: Was bedeutet für dich Privatsphäre?

159 I: Dass meine eigenen Sachen geschützt sind vor anderen, dass ich es nur selbst sehe, außer
160 ich will es anderen zeigen.

161 A: Nehmen wir mal an, der Max ladet sich eine App runter und akzeptiert bei der Installation,
162 dass die App Zugriff hat auf seine Fotos, sein Adressbuch, seinen Kalender und all diese
163 Sachen. Die App speichert alle Informationen, also die ganzen Fotos, alle Nummern, die er
164 im Adressbuch hat. Was meinst du: Wie könnte das für den Max dann aussehen, wenn die
165 Firma all seine Daten hat?

166 I: Dann sieht die Firma genau, was der Max alles tut, was ihn interessiert, wer seine Freunde
167 sind und so.

168 A: Und was kann die Firma dann machen, wenn sie alles über den Max weiß?

169 I: ... sie kann ihm Werbung zuschicken, die sie genau auf ihn anpasst, damit er ja kauft. ...
170 sie könnte ihn erpressen, aber nein, das würde sie wohl eher nicht tun. Ja.

171 A: Hast du dir auch schon mal überlegt einen Dienst oder eine App zu kündigen, weil du
172 gesagt hast, die greifen auf zu viele Daten von mir zu, das kann ich nicht mehr
173 kontrollieren?

174 I: Nein, noch nie.

175 A: Was müsste passieren, dass du eine App löschst oder dich abmeldest und alles gelöscht
176 wird?

177 I: Keine Ahnung, wenn ich auf einmal Fotos von mir im Internet sehe, das wäre ein Punkt,
178 das geht natürlich zu weit. Weil dann können sie auch alles andere von mir veröffentlichen.

179 A: Wie möchtest du dich jetzt in Zukunft vor dieser Datenspeicherung schützen?

180 I: Ja, da sollte ich wohl die, die Sachen, durchlesen die ich akzeptiere. Aber die musst du
181 zuerst einmal verstehen. Ja, das wäre sicher nicht blöd.

182 A: Wie meinst du, sieht unser Leben mit dem Smartphone in 30, 50 Jahren aus?

183 I: Wir werden es noch mehr nutzen und fast alles nur mehr über das Smartphone tun.

184 A: Jetzt sage ich dir ein paar Szenarien und frage dich, ob du das für realistisch hältst:
185 Wenn jemand zum Beispiel täglich sein Smartphone mit Apps und Internet nutzt, wie Twitter
186 und/oder Facebook,, ohne dass er jemals seinen Standort preisgibt. Meinst du, dass es dann
187 dennoch möglich ist, dass man vorhersagen kann, wo sich derjenige in Zukunft aufhalten
188 wird?

189 I: Könnte sein, ja. Weil wenn du heute immer über das Internet zum Beispiel eine Wohnung
190 in Ort 1 suchst, dann ist die Wahrscheinlichkeit groß, dass du dann nach Ort 1 ziehst. So zum
191 Beispiel. Könnte sein.

192 A: Ja, Könntest du dir zum Beispiel auch vorstellen, dass man schon allein von den
193 Informationen, die zum Beispiel Facebook-Freunde veröffentlichen ohne dich dabei zu
194 erwähnen, schon vorhersagen kann, wo du sich befinden wirst in Zukunft?

195 I: Ohne, dass sie mich markieren oder so?

196 A: Ja.

197 I: Ma, das denke ich nicht.

198 A: Ok. Hast du schon mal davon gehört?

199 I: [Schüttelt verneinend den Kopf].

200 A: Wie realistisch ist es für dich, dass die Polizei bereits heute weiß, wo morgen ein
201 Verbrechen stattfindet? Also nicht wer ein Verbrechen begeht, sondern wo. Also zum
202 Beispiel in Ort1 in der und der Gegend.

203 I: Das ist eher unrealistisch denke ich mir.

204 A: Wieso das? Wieso unrealistisch.

205 I: Ja die Polizei hätte dann doch zu viel zu schauen. Ich denke nicht, dass sie das machen.

206 A: Könntest du dir aber vielleicht vorstellen, dass die Polizei, dass sie die Verbrechen von

207 vergangenen Jahren hernimmt und diese auswertet, und dann so Zonen herausfindet, wo viele

208 Verbrechen stattfinden?

209 I: Ma, das denke ich nicht. Nur weil in der Vergangenheit, sagen wir mal an der Kreuzung ein

210 Verbrechen stattfand, muss das deshalb nicht in Zukunft noch einmal passieren.

211 A: Nehmen wir an, eine Frau kauft im Supermarkt verschiedene Sachen ein, aber keine

212 Babysachen, also nichts was man mit einem Baby in Verbindung bringen könnte. Ist es für

213 dich realistisch, dass man dann vorhersagen kann mit relativ hoher Wahrscheinlichkeit, ob

214 diese Frau schwanger ist und in welchem Monat ungefähr?

215 I: Nein, wenn sie gar nichts einkauft und so, denke ich nicht, dass man das sagen kann.

216 A: Denkst du nicht, dass man das zuordnen kann oder so irgendwie?

217 I: Nein.

218 A: Nächstes Beispiel: Ein Mann ist homosexuell aber er gibt das nirgends preis, weder auf

219 Facebook noch sonst irgendwo gibt er an, dass er auf Männer steht. Er sucht auch nirgends

220 nach Sachen, die man mit Homosexuellen in Verbindung bringen könnte. Für wie realistisch

221 ist es für dich, dass eine wildfremde Person, dennoch mit hoher Wahrscheinlichkeit sagen

222 kann, dass dieser Mann homosexuell ist?

223 I: Er sucht im Internet auch nichts?

224 A: Nein, zumindest nichts was mit diesem Bereich in Verbindung gebracht werden kann.

225 I: Eher unwahrscheinlich denke ich mir. Mit dem Internet könnte man das sehen. Außer man

226 sieht wie er geht zum Beispiel und so, vom Verhalten her und wenn er zum Beispiel immer

227 nur mit Männern unterwegs ist. Das kann halt sein, aber wahrscheinlicher ist, wenn man den

228 Verlauf des Internets kombiniert.

229 A: Dass man dann mit der Kombination aller Daten doch was rausfindet?

230 I: Ja, genau.

231 A: Kannst du dir vorstellen, dass, wenn du in Zukunft einen Kredit möchtest, die

232 Kreditinstitute zuerst deine Bewegungsdaten kontrollieren und deine Freundesliste auf

233 Facebook, wenn sie prüfen wollen, welchen Kredit sie dir geben oder ob sie dir überhaupt

234 einen Kredit geben.

235 I: Ja das kann gut sein, überhaupt in der Wirtschaftskrise, dass sie das machen, um

236 sicherzugehen, dass ich kein Geld verliere und dass ich auch alles zurückzahlen kann.

237 A: Hast du davon schon mal gehört?
238 I: Nein.
239 A: Kennst du diese Gesundheits- und Fitnessapp's, wo man eingibt was man isst oder wie viel
240 man trainiert? Wie wahrscheinlich ist es für dich, dass in Zukunft die
241 Gesundheitsversicherungen sich deinen Lebensstil ansehen, was du isst und wie gut du dich
242 bewegst, wenn sie schauen, ob du eine Gesundheitsversicherung bekommst oder nicht.
243 I: Bei uns vielleicht nicht so sehr, aber in anderen Ländern wo das Übergewicht häufiger
244 vorkommt denke ich mir, könnte das schon sein.
245 A: Wieso?
246 Ja, weil das nur Risikofaktoren sind für andere Krankheiten, dann zahlt hier die Kasse nur
247 drauf. Die wollen ja auch nur verdienen.
248 A: Hast du davon schon mal gehört?
249 I: Dass die Apps das machen nicht, nein.
250 A: Für wie realistisch hältst du die Vorstellung, dass man in Zukunft, wenn man
251 beispielsweise auf Google oder auf einer anderen Internetseite ein Wort eingibt oder im
252 Internet oder per SMS etwas schreibt, dass man dann wegen diesem Wort nicht mehr in ein
253 Land einreisen darf
254 I: Ganz sicher nicht.
255 A: Kannst du dir nicht vorstellen?
256 I: Nein.
257 A: Wieso nicht?
258 I: Ich denke mir, da müssten sie alle vorher überprüfen. Ich weiß nicht ob sie das schaffen.
259 A: Es fehlt also an den technischen Möglichkeiten?
260 I: Ja, genau.
261 A: Ist es für dich realistisch, dass man in Zukunft das Verhalten schon vorhersagen kann? Wie
262 du dich verhalten wirst. Aus dem Verhalten der Vergangenheit schon vorhersagen kann, wie
263 du dich in Zukunft verhalten wirst?
264 I: Mit den App's?
265 A: Nein, generell mit ...
266 I: ... Ja, das denke ich schon, weil irgendwie ändert sich der Charakter ja nicht so sehr, dass
267 man sagen kann, vor fünf Jahren, oder vor einem Monaten hat mir das gefallen und jetzt auf
268 einmal nicht mehr.
269 A: Ok, dann hältst du das für realistisch?
270 Ja.

271 A: Hast du davon schon mal gehört?
272 I: Dass man das voraussagen kann?
273 A: Ja.
274 I: Nein.
275 A: Danke für das Interview.

1 **Interview 3, am 22.09.2014. Dauer 28:53 Minuten**

2

3 A: Wie alt bist du und was machst du beruflich?

4 I: Ich bin 22 und bin Beruf 2.

5 A: Mit welchen Medien informierst du dich vorwiegend?

6 I: Mit Internet und die Seiten auch sagen?

7 A: Ja.

8 I: Mit Facebook, Stol [Südtirol Online, Anmerk. der Autorin] und ja Bild.de. Aber vor allem
9 Stol und Facebook.

10 A: Hast du auch Onlinemagazine?

11 I: Ja, genau.

12 A: Nutzt du diese Seiten täglich?

13 I: Jaja.

14 A: Wie sieht es aus mit Radio, Zeitung, Fernsehen?

15 I: Radio beim Autofahren meistens, Zeitung selten, wenn ich gerade mal eine in die Hand
16 bekomm. Fernsehen schon ab und zu.

17 A: Welches Smartphone besitzt du?

18 I: Das Model 5.

19 A: Für was gebrauchst du dein Smartphone?

20 I: Für alles. Ich habe keinen Computer. E-Mails, (...?), für alles.

21 A: Für Fotos?

22 I: Ja.

23 A: Hast du dir auch Apps heruntergeladen?

24 I: Ja, WhatsApp und Facebook. Und so eine Shopping App, hab ich auch. Mehr eigentlich
25 nicht.

26 A: Taschenlampe, Wetter oder so Geburtstagskalender?

27 I: Nein, das hab ich eigentlich nicht heruntergeladen, nein.

28 A: Hast du vom Begriff Big Data schon mal gehört?

29 I: Nein.

30 A: Kannst du dir trotzdem vorstellen, was man darunter versteht?

31 I: (Schüttelt verneinend den Kopf).

32 A: Datenschutz, ist dir das ein Begriff?

33 I: Mhm.

34 A: Wie gut kennst du dich mit Datenschutz aus?

35 I: Eigentlich überhaupt nicht. Also ich bin jemand, der einfach Ok klickt und liest es sich
36 nicht wirklich durch.

37 A: Ok.

38 I: Weil man anders aber nicht dazukommt. Also man muss Ok drücken, sonst kann man es
39 nicht weiter herunterladen, deswegen muss man dort...

40 A: Ok. Erzähl mal: Was weißt du über Datenschutz?

41 I: Grundsätzlich weiß ich wirklich nicht viel. Also ich weiß, dass es um (Veröffentlichung ?)
42 geht, oder jetzt zum Beispiel bei Facebook, dass die Fotos auch wirklich dort bleiben, auch
43 wenn man sie löscht, gehören sie dann Facebook. Mehr habe ich mich damit nie beschäftigt,
44 dadurch, dass mir nie wirklich was passiert ist. Ja.

45 A: Was heißt nie nichts passiert?

46 I: Ich habe jetzt nie einen Virus gehabt, oder nie, dass mich jemand gehackt hat, oder keine
47 Ahnung, was man halt durchaus hört.

48 A: Bist du dir sicher, dass das so ist oder meinst du das?

49 I: Also ich habe noch nichts bemerkt, (lacht) aber es könnte schon sein.

50 A: Datenschutzrichtlinien, ist dir das ein Begriff?

51 I: Nein.

52 A: Datenschutzbestimmung oder Nutzerbestimmung, was man bei den Apps oft so findet?

53 I: Ja, die lese ich dann schon, aber ich stimme immer zu.

54 A: Was meinst denn du, was steht in einer solchen Richtlinie drinnen?

55 I: ... Ja zum einen, dass sie die Daten weitergeben können, oder dass sie über diese verfügen
56 können, dass das ihnen dann gehört wahrscheinlich. Ja recht viel mehr, glaube ich ...Oder.
57 Mein Problem ist, dass ich nicht verstehe, warum, also was sie dann mit diesen Daten tun,
58 weil so interessant bin ich jetzt nicht. (lacht)

59 A: Meinst du, dass deine Apps eigene Datenschutzrichtlinien haben?

60 I: Die, die ich heruntergeladen habe?

61 A: Mhm, oder auch Internetseiten. Haben die eigene, oder alle die gleichen?

62 I: Ich denke schon, dass die eigene haben und ein bisschen abgestimmt sind.

63 A: Du hast gesagt, du hast die Datenschutzrichtlinien noch nie vollständig durchgelesen. Was
64 meinst du haben deine Apps, also Facebook und Co. welche Datenschutzrichtlinien haben
65 die?

66 I: Ich glaube grundsätzlich geht es dann um die Privatsphäre, oder um die Sachen, die man ja
67 auch einstellen kann. Vor allem um das eben, dass man das. Und um die Fotos, das ist das,
68 was ich mir jetzt schon bewusst bin, dass wenn ich etwas reinstelle, dass auch, wenn ich es

69 lösche, dass es dann immer wieder verwendet werden kann. Aber grundsätzlich um die
70 Privatsphäre, die Daten, die du jetzt eingibst. Aber ich bin jetzt nicht jemand, der alles
71 kommentiert.

72 A: Das heißt, dass sie das Recht haben, alles von dir zu verwenden, ohne Schutz so zu sagen,
73 oder in dem Maße, wie es in der Richtlinie steht?

74 I: Ja.

75 A: Wo kann man sich denn über die Datenschutzrichtlinien informieren, jetzt zum Beispiel
76 von den Apps?

77 I: Ja, da kann man sich dann nur das Ding durchlesen, wahrscheinlich, was ja immer kommt.
78 Aber es gibt sicher eine Seite, wo man sich das durchlesen kann. Das müssen sie sicher
79 angeben, kann ich mir vorstellen, dass man das muss, aber ich glaube, wenige lesen sich das
80 dann durch.

81 A: Ja, das ist dann eine andere Sache.

82 I: Aber sie müssen es sicher angeben.

83 A: Auf welche Daten meinst du können deine Apps zugreifen?

84 I: Ich glaube, also das, was ich jetzt auch so gehört habe, das war jetzt ja Thema. Glaub ich
85 grundsätzlich auf alles, also ja.

86 A: Was ist alles?

87 I: Ja, alles. Handynummer, Nachrichten, man hat ja gehört, dass sie jetzt wirklich auch im
88 Stande sind, die Nachrichten, die E-Mails, dass sie das wirklich mehr oder weniger lesen.

89 A: Wo hast du das gehört?

90 I: Im Fernsehen haben sie das jetzt mal berichtet. Bei den Promis halt, aber auch sonst bei den
91 [normalen Menschen], ja.

92 A: Das heißt sie können auf alles, was du auf dem Handy hast, zugreifen, oder nur auf
93 bestimmte Bereiche?

94 I: Nein, also, so wie ich das verstanden habe, auf die Apps, die man sich runterladet, auf die
95 vor allem.

96 A: Das heißt sie können auf die App zu greifen, oder die App kann zugreifen?

97 I: Nein, auf die App. Was ich weiß, aber ich bin da jetzt nicht so... Aber da gibt es sicherlich
98 auch eine Hintertür, wo man auch auf die privaten Nachrichten zugreifen kann, weil so wie
99 ich das verfolgt habe, konnten sie dann auch auf die privaten Nachrichten zugreifen und das
100 wär jetzt ja nicht unbedingt auf der App gewesen, also...

101 A: Das heißt im Grunde ist das gesamte Handy von dir offen.

102 I: Ja.

103 A: Du hast gesagt du nutzt auch die Fotokamera auf deinem Smartphone.
104 I: Ja.
105 A: Nehmen wir mal an, die Anna nützt ihr Handy immer nur zu Hause, alleine, ohne, dass
106 sich jemand um sie herum aufhält. Sie macht auch Fotos mit ihrem Handy. Meinst du, dass es
107 möglich ist, dass jemand diese Fotos sehen kann, ohne dass sie jemandem das Handy gibt, es
108 zeigt, oder schickt?
109 I: Ich glaube schon.
110 A: Wieso?
111 I: Ja, weil ich eben. Also es ist so, ich bin jemand, der ziemlich offen mit diesen Sachen
112 umgeht. Also ich bin nicht jemand, der sich diese Bestimmungen durchliest, aber
113 grundsätzlich denk ich mir, dass es für die Privatsphäre oder die Fotos und so auf dem Handy
114 nicht so vorteilhaft ist. Also ich denk mir, dass es da schon irgendeinen Weg gibt.
115 A: Könntest du dir auch vorstellen welchen Weg?
116 I: Nein. Aber ich kann mir vorstellen, dass es da einen Weg gibt, dass man auf das Handy
117 zugreifen kann.
118 A: Könntest du dir vorstellen, dass man das ihnen sogar erlaubt, unbewusst? Also, dass sie
119 sogar die Erlaubnis haben, aber man selbst das eigentlich nicht weiß?
120 I: Ja, jaja, das glaub ich schon.
121 A: Wie gut sind deine Fotos auf deinem Smartphone geschützt?
122 I: Eigentlich habe ich gar nichts. Also ich habe nichts eingestellt, also denke ich nicht gut.
123 A: Würdest du da was verändern?
124 I: Ja, wenn ich wüsste wie, schon.
125 A: Wer bestimmt über die Sicherheit deiner Daten auf deinem Handy?
126 I: Ja grundsätzlich müsste ich das machen. Aber wer, das weiß ich nicht.
127 A: Ok, und wie kannst du das kontrollieren, oder kannst du das überhaupt kontrollieren, wer
128 da zugreift?
129 I: Also ich kann das nicht kontrollieren, nein. Aber wenn man sich mit dem Thema ein
130 bisschen beschäftigt, dann wüsste man wahrscheinlich wie. Das gibt es sicher irgendwo
131 nachzulesen oder so.
132 A: Wer außer dir, meinst du hat noch Zugriff auf deine Fotos, deine Kalendernotizen, dein
133 Adressbuch usw.?
134 I: Keine Ahnung. Es gibt sicher so ein System, aber wer, also einen Namen oder so kann ich
135 dir jetzt nicht sagen.
136 A: Und wenn du jetzt an deine Apps denkst.

137 I: Ja diese App selber, also Facebook auf Facebook, WhatsApp auf WhatsApp, mittlerweile
138 ist das ja auch Facebook, da hat man ja auch so einen Trubel gehört über diese Daten, ja
139 einfach jede App.

140 A: Wenn wir jetzt deine Apps hernehmen. Auf welche Bereiche können die dann zugreifen,
141 hast du da eine Ahnung?

142 I: Da stellt man ja immer ein, auf die Infos und so, auf die auf jeden Fall, und wie gesagt, ich
143 bin dann überzeugt, dass man das dann sicher noch erweitern kann.

144 A: Auf die Infos, heißt dein Name?

145 I: Auf den Namen, die E-Mailadresse, auf alles, was du angibst dann.

146 A: Dann können sie auf Fotos und Adressbuch auch zugreifen?

147 I: Nein.

148 A: Wie meinst du erhalten die den Zugriff überhaupt?

149 I: Ja durch die Zustimmung von uns. eigentlich.

150 A: Wieso meinst du brauchen Apps Zugriff auf diese Bereiche?

151 I: Ja eben, das ist ja die Frage. Bei Promis oder so, verstehe ich es, aber bei so normalen
152 Personen...

153 A: Was meinst du, welche Daten braucht denn die App, damit sie überhaupt funktionieren
154 kann?

155 I: E-Mail und ich weiß das jetzt nicht mal so genau, weil ich muss ehrlich sagen, diese Apps
156 hat mir Person 3 heruntergeladen. Aber E-Mail ist immer etwas, das man angeben muss, und
157 Name, Handynummer, nein Handynummer gar nicht, Kreditkarte muss man angeben, wenn
158 etwas zu zahlen ist. Wobei, wenn es zu zahlen ist, dann gebe ich die Kreditkartennummer
159 nicht an, dann lass ich es meistens.

160 A: Könntest du dir vorstellen, dass zum Beispiel eine Wetter App Zugriff auf das Internet
161 braucht um funktionieren zu können?

162 I: Ja.

163 A: Wie sieht es mit der Kamera aus? Dass sie Zugriff auf deine Kamera hat?

164 I: ... Ja, kann ich mir vorstellen, dass sie das braucht.

165 A: Und der Zugriff auf dein Adressbuch? Die Wetter App?

166 I: Grundsätzlich ja, eigentlich bräuchte sie das nicht, aber ich denke mir schon, dass sie das
167 haben könnte durch die Bestimmungen, dass sie das Recht hat dort zuzugreifen.

168 A: Wie sieht es mit den Fotos aus?

169 I: Gleich.

170 A: Wieso meinst du holt sich die App die Erlaubnis auf den Zugriff aufs Internet, Foto,
171 Adressbuch, Kamera, was nutzt ihr das?

172 I: Für irgendwas wird sie das schon brauchen, oder ausnutzen, keine Ahnung. Dass die App
173 nicht die sicherste Variante ist, oder dass auch auf Facebook das nicht so sicher ist, oder dass
174 man sagt, man soll nicht unbedingt die Handynummer reingeben, das ...

175 A: Ausnutzen, wie meinst du das?

176 I: Ja man hört ja immer wieder mal von Hackern und so. Aber jetzt für was genau und warum,
177 das weiß ich nicht. Ich glaub die App selbst hat keinen Nutzen davon, wenn, dann ist es
178 jemand im Hintergrund, der sich vielleicht Daten herunterlädt oder so.

179 A: Also könntest du dir vorstellen, dass über deine App Daten heruntergeladen werden?

180 I: Ja, das kann ich mir schon vorstellen.

181 A: Und was macht der im Hintergrund mit diesen Daten dann?

182 I: Keine Ahnung. (lacht). Jetzt wenn ein Telefonbuch oder Adressbuch von jemand anderem
183 genommen wird, ist logisch jetzt nicht soo, weil immerhin eine Handynummer ist etwas, das
184 ich nicht hergebe. Also das ist bei mir auch nirgends drinnen.

185 A: Du hast ja gesagt, dass die App Informationen kopiert und speichert. Was meinst du, kann
186 ein Unternehmen machen, wenn es von unzählig vielen Leuten ganz, ganz viele Daten hat?

187 I: Was sie damit machen?

188 A: Ja.

189 I: Jetzt, ausnutzen, ich weiß nicht, was sie damit machen können. Überprüfen, ja bo, das nützt
190 ihnen ja auch nicht viel, wenn sie diese haben, was sollen sie mit denen?

191 A: Und welche Folgen könnte das für uns haben?

192 I: Dass wir überhaupt keine Privatsphäre mehr haben, dass wir immer überwacht werden, also
193 immer kontrolliert werden können wo wir sind und was wir machen. Und dass sie dann, der
194 nächste Schritt ist dann, dass es bis zu Bankdaten, Kreditkarteninformationen und
195 Handynummern dann auch nicht mehr weit ist, dass man halt überhaupt nichts mehr schützen
196 kann, dass man eigentlich ein offenes Buch ist.

197 A: Nehmen wir mal an, die Anna lädt sich eine App runter und akzeptiert bei der Installation,
198 dass die App überall zugreifen kann, auf Fotos, Adressbuch, Kalender und alles weitere. Die
199 App speichert dann alle Informationen, welche die Anna auf ihrem Smartphone hat. Was
200 meinst du: Welche Folgen könnte das für die Anna haben, wenn die App jetzt alles weiß.
201 Alles, also die Daten, die sie auf dem Handy hat, sehen kann?

202 I: Ja, angenehm ist das natürlich nicht. Folgen, ja eben überwacht sein, dass man nicht mehr
203 das tun kann, was man eigentlich will, jetzt in der Hinsicht, dass zum Beispiel, wenn man eine

204 SMS schreibt, möchte man, dass das nur unter zwei Personen bleibt und nicht dass zehn
205 andere mitlesen. Die Privatsphäre, die man sich eigentlich wünscht, dass nicht alles öffentlich
206 ist, dass diese wirklich öffentlich gemacht werden kann.

207 A: Könntest du dir vorstellen, dass man sich dann anders verhält, wenn man weiß, da liest
208 jemand mit?

209 I: Ja, das denke ich schon.

210 A: Ist das für dich ein Einschnitt in deine Privatsphäre und in dein Verhalten?

211 I: Ja! Also wenn ich jetzt wüsste, dass andere mitlesen, was wahrscheinlich so ist, zum
212 Beispiel bei Facebook, da weiß ich ja, das das so ist, dann ist das schon anders, ja.

213 A: Wie verhältst du dich dann?

214 I: Ja jetzt, eher, ich tu dann weniger posten oder, ich bin grundsätzlich nicht jemand der alles
215 reinstellt, also Fotos schon, aber ich mag zum Beispiel nicht, wenn man schreibt wo man
216 gerade ist. Das mag ich überhaupt nicht, dass jeder weiß wo ich gerade bin, das kann man ja
217 eingeben mit dem Standort und so. Handynummer würde ich auch nie reinstellen, wobei mir
218 die E-Mailadresse eigentlich schon zu viel ist, aber die ist, ja. Eben, wenn man sich anmeldet,
219 denkt man oft nicht an die Sachen.

220 A: Hast du dir schon mal überlegt Dienste oder Apps aufzugeben, wenn sie die Erlaubnis
221 brauchen auf deine Bereiche?

222 I: Mhm. Ja, wie gesagt, ich hab nicht so viele Apps und genau aus diesem Grund eigentlich
223 auch. Also das ist schon der Grund. Also WhatsApp ist etwas, das mir passt und Facebook ist
224 mittlerweile ja ... schon fast zur Sucht geworden, wobei ich war schon mal abgemeldet.

225 A: Wieso das?

226 I: Weil mir es damals nicht mehr gepasst hat, immer zu schreiben und zu schauen, aber dann
227 hat es sich wieder eingebürgert.

228 A: Aber aus den Gründen, weil es dir nicht gepasst hat?

229 I: Ja, damals war ich das nicht gewohnt, dass da im Grunde jeder Freundschaftsanfragen
230 machen kann und jeder sieht die Fotos dann und ja.

231 A: Kennst du jemand der das noch gemacht hat?

232 I: Abgemeldet?

233 A: Ja.

234 I: Ja, Freunde.

235 A: Aus welchen Motiven haben sie das gemacht?

236 I: Aus denselben.

237 A: Was muss passieren für dich, dass du sagst WhatsApp oder Facebook gibst du wirklich
 238 auf?

239 I: Ja, da muss ich schon ein Foto von mir sehen, oder auf ein Mal, dass mir auf dem Handy
 240 fremde Personen schreiben, oder dass ich merke, dass jemand in mein Profil reinkommt oder
 241 dass auf einmal Nachrichten verschickt werden.

242 A: Das Gefühl von Unsicherheit zu haben?

243 I: Ja genau, dann würde ich es sicher lassen.

244 A: Wie möchtest du dich in Zukunft vor der Datenspeicherung schützen?

245 I: Ja, also das habe ich mir schon jetzt mal überlegt, dass ich auf Facebook die Privatsphäre,
 246 die Einstellungen verbessern möchte. Ja grundsätzlich wäre dann sicher der gesamte
 247 Datenschutz mal zu lesen, es ist nur so enorm viel und das machen sie wahrscheinlich auch
 248 extra und extra klein gedruckt, damit man sich das ja nicht durchliest, weil, wenn man es sich
 249 durchlesen würde, würde man es wahrscheinlich nicht mal mehr bestätigen, kann ich mir
 250 vorstellen. Deswegen wäre das sicher ein Punkt, den man sich überlegen müsste. Ich bin aber
 251 nicht jemand, der sich enorm viele Apps herunterladet, erstens, weil ich dann viel zu viel
 252 Angst hätte irgendwo angemeldet zu sein, wo ich nicht angemeldet sein möchte.

253 A: Wie meinst du ist unser Leben in 30, 50 Jahren mit dem Smartphone, mit dieser
 254 Technologie?

255 I: Ja, ziemlich verstrahlt. (lacht). Also ich denke es wird noch viel mehr über das Smartphone
 256 gehen, es ist ja jetzt schon viel. Ich mag ja nur mich anschauen, ich mach alles über das
 257 Handy, ich hab es immer dabei. Man wird ja schon fast nervös, wenn man es nicht mehr dabei
 258 hat. Ich hab mir jetzt fest vorgenommen Tage einzulegen, an denen ich das Handy weggebe.
 259 Es ist dann aber auch mit dem Beruf schwierig [um die Identität der Interviewpartnerin zu
 260 schützen, wird diese Passage über ihren persönlichen Alltag nicht transkribiert], wobei ich mir
 261 denke, es ist viel Einstellungssache und auch eine organisatorische Sache, der man sich
 262 stellen könnte. In Zukunft wird sicher noch mehr gemacht und in Zukunft wird es sicher noch
 263 unsicherer, wie es jetzt bereits ist.

264 A: Jetzt sage ich dir ein paar Szenarien und frage dich für wie realistisch du das hältst:
 265 Wenn jemand täglich sein Smartphone mit Apps und Internet nutzt, zum Beispiel auch
 266 Twitter und/oder Facebook,, ohne dass er jemals seinen Standort preisgibt und es auch
 267 nirgends aufscheinen lässt. Ist es für dich realistisch, dass es dann dennoch möglich ist, dass
 268 mit einer großen Wahrscheinlichkeit vorhersagbar ist, wo sich derjenige in Zukunft aufhalten
 269 wird?

270 I: Ja.

271 A: Wieso?

272 I: Ich denke mir beim Internet, oder grundsätzlich das gesamte System unterschätzen wir, auf
273 wie viel das eigentlich zugreifen kann. Auch das Handy selbst kann man schon orten. Also
274 ich denke schon, dass das möglich ist.

275 A: Und wenn du jetzt davon ausgehst, dass das Handy nicht geortet werden könnte und zum
276 Beispiel auch keine Informationen über „Hinterwege“ herausgefunden werden könnten,
277 glaubst du dann trotzdem, dass das so sein kann?

278 I: Ich denke schon, aber warum, ich denke einfach, dass auch, wenn es jetzt kein Schlupfloch
279 gibt, dass es grundsätzlich einfacher ist, als wir uns das vorstellen können, weil nicht umsonst
280 kommen so viele Sachen ans Tageslicht.

281 A: Eine genaue Begründung hast du aber nicht?

282 I: Nein.

283 A: Hast du davon schon mal gehört?

284 I: Mit Standort und so?

285 A: Ja.

286 I: Gehört, das speziell jetzt nicht. Aber dass man oft Sachen grundsätzlich sonst hernehmen
287 kann, oder, dass man sagt, derjenige hat jetzt auf meine Seite zugegriffen, ohne, dass er sonst
288 was über mich gewusst hat schon, ja.

289 A: Wie meinst du zugegriffen?

290 I: Ja, entweder auf das Profil gekommen ist, oder, dass es möglich ist aufs Handy zuzugreifen
291 durch die App, dass man dadurch auch auf das Telefonbuch kommt und so.

292 A: Ok. Ist es für dich realistisch, dass die Polizei heute schon wissen kann wo morgen ein
293 Verbrechen stattfindet? Also nicht wer, sondern wo.

294 I: (lacht) Wenn sie das wissen würden, würden sie wahrscheinlich schon vorher was machen.
295 Ich denke nicht, aber in der Zukunft vielleicht.

296 A: Ok, aber jetzt im Moment noch nicht?

297 I: Nein, denke ich nicht.

298 A: Wieso nicht?

299 I: Ja, weil ich mir einfach denke, wenn das so wäre, dann könnte man viel vorbeugen. Außer
300 sie sind zu faul nachzuschauen. (lacht)

301 A: Das heißt dann für dich, dass es schon möglich wäre.

302 I: Es wäre vielleicht sicher mal möglich.

303 A: Sicher einmal heißt in Zukunft oder jetzt auch schon?

304 I: Ich denke in Zukunft. Ich denke in Zukunft.

305 A: Hast du davon schon irgendwann mal was gehört?

306 I: Nein.

307 A: Dann, Szenario drei: Nehmen wir an, eine Frau kauft im Supermarkt verschiedene Sachen

308 ein, aber keine Babysachen, also nichts was man mit einem Baby in Verbindung bringen

309 könnte. Könntest du dir vorstellen, dass man nur von den Artikel, die sie kauft, sagen kann,

310 ob sie schwanger, oder nicht, und wann ungefähr der Geburtstermin ist? Also es sind

311 alltägliche Sachen.

312 I: Aber hat sie ihre Daten angegeben?

313 A: Nein.

314 I: Nichts?

315 A: Nein, nur die gekauften Artikel, auch keine Vorteilskarte oder so.

316 I: Hat sie mit Bankomat gezahlt?

317 A: Auch nicht, ganz normal.

318 I: Nein, das glaube ich nicht.

319 A: Wieso?

320 I: Ja nein, weil, eben wenn jetzt Daten da wären oder so, oder wenn sie mit Bankomat zahlen

321 würde, vielleicht könnte man es dann zurückführen, oder mit der Kreditkarte oder so, aber

322 grundsätzlich denk ich das jetzt nicht, nein.

323 A: Ok, dann nehmen wir an, ein homosexueller Mann nutzt viel das Internet, unter anderem

324 auch Social Media, aber gibt nirgends an, dass er auf Männer steht. Er hält sein Sexualleben

325 geheim und gibt es nirgends preis. Könntest du dir dann vorstellen, dass eine wildfremde

326 Person, dennoch mit hoher Wahrscheinlichkeit sagen kann, dass dieser Mann homosexuell

327 ist?

328 I: Ja, das denk ich schon.

329 A: Wieso?

330 I: Ja, weil man sich ja doch oft ertappt, dass man einen kleinen Hinweis oder irgendwas gibt.

331 A: Was wäre zum Beispiel ein kleiner Hinweis?

332 I: Ja es mag ja auch schon ein Foto sein, oder ... irgendeine Seite im Internet.

333 A: Und wenn er das jetzt nicht machen würde, solche „Extra“-Seiten im Internet ansehen.

334 I: Wenn er es sonst nirgends angibt? Und diese Person kennt ihn nicht. Ja ich weiß nicht,

335 grundsätzlich denke ich mir kann man das. Wobei es ist ziemlich schwierig das

336 nachzuweisen. Ich hätte es eben über Internetseiten oder solche Seiten für möglich gehalten,

337 dass man das zurückverfolgen kann. Aber sonst glaub ich nicht.

338 A: Weil es zu schwierig ist?

339 I: Ja, wenn jemand das jetzt wirklich herausfinden möchte, dann kommt er sicherlich auf
340 einen Weg, auf dem er es herausfindet. Ja.

341 A: Und wie bzw. könntest du dir vorstellen, was er da tun müsste?

342 I: Ja, dann müsste es zumindest ein Foto geben, oder dass er durch Bekannte zu dem kommt,
343 wo er drauf ist, durch Hintertüren wiederum.

344 A: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft, wenn sie einen Kredit vergeben
345 wollen, zuerst die Bewegungsdaten und die Freundesliste von verschiedenen Seiten
346 kontrollieren, wenn sie prüfen wollen, ob jemand kreditwürdig ist oder nicht?

347 I: Ja.

348 A: Wieso?

349 I: Weil ich eben denke, dass so. Man kann, wenn man sich so sieht, ziemlich verstellen, aber
350 wenn man dann schauen kann auf welchen Seiten jemand ist oder mit wem man sich umgibt
351 recht viel herausfinden. Ich denk schon, dass das mal sein wird, wenn es nicht schon so ist,
352 dass sie wirklich schauen.

353 A: Hast du davon schon mal gehört?

354 I: Nein gehört jetzt direkt nicht, aber der Vater vom Person 3 hat gesagt, dass sie da schon oft
355 im Internet schauen.

356 A: Also hast du schon davon gehört?

357 I: Ja, gehört, er hat gesagt, das werden sie jetzt langsam einführen.

358 A: Kennst du diese Gesundheits- und Fitnessapp's, wo man eingibt was man isst oder wie viel
359 man trainiert? Meinst du, dass in Zukunft Gesundheitsversicherungen prüfen, ob du dich
360 gesund ernährst und dich ausreichend bewegst, wenn sie schauen, welche Versicherung du
361 bekommst, oder ob du überhaupt eine Versicherung bekommst?

362 I: Ja, ich denke mir eben, grundsätzlich kann das eine Zukunftsvision sein, was, denke ich,
363 aber erst im Wachsen ist.

364 A: Ok. Wieso hältst du das für möglich?

365 I: Weil ich eben grundsätzlich denke, dass die Menschen nicht mehr ein so großes Vertrauen
366 in jemanden haben wie es früher vielleicht einmal war und mehr auf Fakten und Daten gehen.
367 Und so eine App ist natürlich etwas, wo sie sagen können, hier ist ein Beweis, wo sie eine
368 Studie machen können und sehen, ob jemand wirklich so gesund ist, wie sie angibt oder
369 täuscht sie das nur vor. Ja.

370 A: Für wie realistisch hältst du es, dass wenn man zum Beispiel im Internet oder in einer
371 Nachricht ein paar Wörter schreibt, so bestimmte Wörter, dass man dann in ein Land nicht
372 mehr einreisen darf, weil man das geschrieben hat?

373 I: Ja ziemlich. Also Amerika ist da ja Vorzeigeland, oder –Staat, was sich wirklich ziemlich...
374 Also bei ihnen muss man sich ja anmelden, dass sie wissen, dass du kommst und im
375 Reisebüro haben sie auch gesagt, da wird wirklich kontrolliert. Ob sie auch auf Wörter
376 schauen, weiß ich jetzt nicht, aber wenn jetzt jemand auffällt, glaub ich schon, dass das was
377 sein könnte, ja. Was ich aber auch gut finde, wenn sie es wirklich so machen würden.
378 A: Wieso? Nicht wieso, dass du es gut findest, sondern wieso glaubst du, dass es wirklich so
379 ist?
380 I: Ja einmal, weil sich der Terrorismus verbreitet hat auch und jedes Land will sich schützen
381 und auch die Bevölkerung schützen, denk ich mir, und dass sie durch das einfach mehr
382 schauen. Aber da ist auch wieder, über Facebook oder über das Internet sind die Leute oft
383 ganz anders, als wie wenn man die Leute so kennenlernt. Sie getrauen sich viel, viel mehr und
384 da findet man dann auch oft Sachen heraus.
385 A: Hast du davon schon mal gehört, oder bist du damit in Berührung gekommen, weil du
386 gesagt hast Reisebüro?
387 I: Die im Reisebüro hat eben gesagt, dass in Amerika das so ist. Jetzt ob sie wirklich so genau
388 schauen, ich denke mir, wenn nur so jemand, wie Person 3 und ich, würden sie vielleicht nicht
389 kontrollieren, aber wenn jemand vielleicht von Israel oder so einem Land heranreist, könnte
390 sein, dass sie denjenigen mehr kontrollieren.
391 A: Wenn wir zwei jetzt zum Beispiel nach Amerika fahren würden und ich schreiben würde:
392 „In Amerika wird es rund gehen, wir werden Amerika zerstören.“, meine damit aber eine
393 Party, nicht uns selbst. Meinst du, wäre das dann so ein Grund, dass sie uns aufhalten und
394 nicht einreisen lassen würden?
395 I: Ich denke, da wird dann schon das Ganze berücksichtigt. Ich denke es hat auch viel mit
396 Klischee zu tun, weil bei zwei Mädchen sehen sie vielleicht nicht eine so große Gefahr, aber
397 ich denke schon, dass das zur Zukunft ein bisschen dazugehört, dass das kontrolliert wird.
398 Also wenn jetzt mal jemand schreibt, eben: Es wird rundgehen und wir zerstören Amerika,
399 dann, ich denke mir, dann schauen sie sich schon alles an, oder dass eine Meldung rausgeht
400 oder keine Ahnung, jetzt das ganze System kann ich dir nicht erklären, aber ich denke schon,
401 dass das in Zukunft so kommen wird.
402 A: Kannst du dir das jetzt, heute, oder auch in der Vergangenheit auch schon vorstellen?
403 I: Ich kann mir das schon vorstellen, aber ich denke, dass sie noch mehr darauf zugreifen
404 werden.
405 A: Also das heißt, es ist schon so, aber es wird noch viel mehr ausgebaut?

406 I: Ja ich denke schon, dass wir das nicht so bewusst wahrnehmen, aber ich denke schon, dass
407 es so ist, ja.

408 A: Kannst du dir vorstellen, dass man aus dem Verhalten der Vergangenheit, das Verhalten in
409 der Zukunft schon vorhersagen kann?

410 I: Ja, das kann ich mir schon vorstellen.

411 A: Wieso?

412 I: Ja, weil ein Mensch ändert sich nicht von heute auf morgen, sicher, man ändert sich schon,
413 aber dann muss man diese Faktoren auch berücksichtigen. Aber so grundsätzlich, wenn man
414 sieht, der war sein ganzes Leben lang so und hat sich so verhalten, wird er sich sehr
415 wahrscheinlich auch morgen noch so verhalten, wie die letzten 25 Jahre.

416 A: Hast du davon schon mal gehört?

417 I: Nein, so genau nicht.

418 Danke für das Interview.

1 **Interview 4, am 23.10.2014. Dauer 21:33 Minuten**
2
3 A: Wie alt bist du, und was machst du beruflich?
4 I: Ich bin 24 Jahre alt und Beruf 3.
5 A: Mit welchen Medien informierst du dich vorwiegend?
6 I: Ja, Medien versuche ich ein bisschen zu meiden. Bei uns lese ich ab und zu die Zeitung 1,
7 und manchmal schau ich auch die Nachrichten im Fernsehen.
8 A: Und Radio?
9 I: Radio hör' ich eigentlich täglich und ja, über das Handy.
10 A: Was nutzt du beim Handy?
11 I: Ja, Facebook, WhatsApp.
12 A: Hast du auch oft so Onlineseiten, dass du zum Beispiel bei Facebook Aktualisierungen
13 bekommst?
14 I: Ja, da habe ich halt die Stol, die Zeitung 1, aber sonst eigentlich nicht.
15 A: Das machst du täglich?
16 I: Ja.
17 A: Welches Smartphone besitzt du?
18 I: Das Model 6.
19 A: Für was brauchst du dein Smartphone?
20 I: Ja eigentlich nur fürs Schreiben und fürs Telefonieren, aber jetzt, wenn du Internet auch hast, nutzt
21 du halt das Internet auch, wie Facebook und andere Sachen halt.
22 A: Und Foto, Wecker?
23 I: Ach ja, Foto, Wecker, die Kamera einfach, Spiele oft auch.
24 A: Kalender oder Memos oder so?
25 I: Kalender weniger, Geburtstagskalender halt.
26 A: Hast du auch Apps heruntergeladen auf dein Smartphone?
27 I: Ja, hab ich.
28 A: Welche?
29 I: Ja ein paar Spiele hab ich, Facebook ist heruntergeladen, WhatsApp, was denn noch?
30 Kamera eine.
31 A: Kamera?
32 I: Ja, eine Kamera Fotos zu machen.
33 A: War das noch nicht drauf auf dem Smartphone?

34 I: Doch, war schon, aber das ist eine, die die Fotos ein bisschen bearbeiten kann mit Farben
35 und Panoramafunktion.

36 A: Taschenlampe war schon drauf?

37 I: Ja, Taschenlampe war schon, Wetter ist auch schon drauf gewesen.

38 A: Wie oft verwendest du diese Apps?

39 I: Ja, ein paar täglich, ein paar nur ein Mal das Monat, ein paar nur ein Mal die Woche.

40 A: Welche verwendest du selten?

41 I: Ja, die Kamera, mit der ich Fotos aufnehmen kann und bearbeiten, selten, ein Mal in der
42 Woche die Spiele und täglich ist halt Facebook und WhatsApp oder den Wecker oder so, das
43 ist halt täglich.

44 A: Hast du den Wecker auch heruntergeladen?

45 I: Nein, der war schon drauf.

46 A: Hast du schon einmal den Begriff Big Data gehört?

47 I: Nein.

48 A: Kannst du dir dennoch vorstellen, was das ist?

49 I: Das hat sicher was mit dem Datenschutz zu tun, und big, groß, denk ich mir.

50 A: Ok, also großer Datenschutz?

51 I: Ja, sowas denk ich mir.

52 A: Datenschutz als Begriff ist dir bekannt?

53 I: Ja, ist mir ein Begriff, ja.

54 A: Wie gut kennst du dich mit Datenschutz aus?

55 I: Ja, ein bisschen, jetzt aber nicht, ich bin sicher kein Profi darin.

56 A: Erzähl mal, was weißt du, oder was ist für dich Datenschutz?

57 I: Ja, einfach Datenschutz, wenn du irgendwo, sagen wir mal bezüglich Internet, deine Daten
58 irgendwo eingibst. Von den Firmen kommt immer dann, dass die Daten geschützt werden, die
59 du ihnen gibst.

60 A: Ist das nur auf das Internet bezogen?

61 I: Nein, generell. Also auf alles. Auf Firmen, auf jegliche, wo du eine Dienstleistung hast und
62 Daten abgeben musst, müssen sie, musst du es meistens unterschreiben oder bestätigen sogar.

63 A: Also Datenschutzlinie, ist dir ein Begriff?

64 I: Ja.

65 A: Die musst du dann unterschreiben?

66 I: Ja.

67 A: Hast du schon mal eine unterzeichnet?

68 I: Ja, ein paar sicher.
69 A: Ok, hast du dir auch schon mal eine durchgelesen?
70 I: Nein, ganz im Detail nie, nein.
71 A: Was genau regelt die Datenschutzrichtlinie?
72 I: Ich weiß, eine, die ich mir durchgelesen habe, dass sie eventuell, wenn es nötig ist, die
73 Daten verwenden kann, aber dass sie sonst auch um Erlaubnis fragen müssen, ob sie deine
74 Daten verwenden können.
75 A: Wenn wir nun an deine Apps denken. Meinst du haben diese eigene
76 Datenschutzrichtlinien?
77 I: Sicher, andere halt. Im Grund denk ich mir, ein Teil wird sicher gleich sein müssen und
78 sicher werden sie sie abändern können, wie viel sie verwenden können und welche Daten sie
79 verwenden können.
80 A: Wo meinst du, kann man sich über diese Datenschutzrichtlinien informieren?
81 I: In welchem Amt oder wie?
82 A: Von der App zum Beispiel, oder von der Internetseite.
83 I: Ja sicher bei dieser Firma denk ich mir.
84 A: Und wo genau?
85 I: Also bei der App gibt es schon Einstellungen, wo ich die Daten selber einrichten kann.
86 A: Bei der App selbst, wenn du sie öffnest?
87 I: Ja. Und sonst findet man sie sicher dort irgendwo bei den Einstellungen oder so.
88 A: Von der App?
89 I: Ja.
90 A: Wenn wir uns nun deine Apps ansehen, weißt du, welche Datenschutzrichtlinien deine
91 Apps haben?
92 I: Genau weiß ich es nicht. Die sind meistens so lang, da ist immer nur zu akzeptieren.
93 A: Hast du dir eine halbwegs durchgelesen oder überflogen?
94 I: Jetzt von den Apps keine.
95 A: Auf welche Daten können deine Apps zugreifen auf deinem Smartphone?
96 I: Wie meinst du das?
97 A: Ja. Können Apps auf deinem Smartphone zum Beispiel auf deine Fotos, deine
98 Kontaktdaten im Adressbuch, deinen Kalender usw. zugreifen?
99 I: Nein.
100 A: Kontrollierst du das?
101 I: Ja.

102 A: Wie kontrollierst du das?

103 I: Ja, wenn sie sich zum Beispiel mit dem Internet verbinden möchten, verweigere ich es.

104 A: Glaubst du, dass deine Apps irgendwelche Daten von dir brauchen, damit sie funktionieren

105 können?

106 I: Nein! Nein, nein, ich glaub, ... ja und nein. Damit die App funktionieren kann?

107 A: Ja.

108 I: Im Endeffekt glaube ich nicht so sehr.

109 A: Und glaubst du sie brauchen speziellen Zugriff auf etwas, damit sie funktionieren können?

110 I: Nein, es ist, wenn du dich irgendwo registrieren musst, dann brauchen sie ja Daten, weil

111 wie willst du sonst jemanden registrieren, aber jetzt bei Spiele musst du dich nicht

112 registrieren, deshalb ist das sicher eigentlich nicht.

113 A: Wenn du zum Beispiel eine Spiele-App hast und die sagt sie braucht Internetzugriff, damit

114 sie funktionieren kann, ...

115 I: Dann nehme ich diese gar nicht.

116 A: Ok, könntest du dir aber vorstellen, dass eine Spiele-App sagt, sie braucht Internetzugriff?

117 I: Ja, sicher.

118 A: Wie sieht es mit Video- und Fotokamera aus?

119 I: Das kann man auch einstellen.

120 A: Aber du könntest dir theoretisch vorstellen, dass die App sagt, sie braucht den Zugriff,

121 damit sie funktionieren kann.

122 I: Ja.

123 A: Was ist, wenn eine Spiele App, oder irgendeine App sagt, sie braucht Zugriff auf dein

124 Adressbuch, damit sie funktionieren kann.

125 I: Nein, dann tue ich das auch nicht.

126 A: Kannst du dir das aber vorstellen, dass es das gibt?

127 I: Ja, geben tut es diese Apps sicher.

128 A: Kontrollierst du das dann auch, weil du sagst das, tust du nicht.

129 I: Ja.

130 A: Wie kontrollierst du das?

131 I: Wenn ich verbunden werde oder wenn, oft kommt eine Meldung auch, dass man sich

132 verbinden muss, dann verbinde ich mich nicht.

133 A: Kannst du dir auch vorstellen, dass sich die App, ohne dich zu fragen, verbindet?

134 I: Nein. Nein, das muss sie mich sicher fragen.

135 A: Könntest du dir aber vorstellen, dass du ihr zum Beispiel bei der Installation, in den
136 Datenschutzrichtlinien, schon erlaubt hast, dass sie auf das Internet zugreifen darf, wenn sie
137 es benötigt?

138 I: Achso, hm, ja das könnte sein.

139 A: Wieso, meinst du, braucht eine App Zugriff auf verschiedene Bereiche?

140 I: Ja zum einen, damit sie funktioniert, wenn ich zum Beispiel die Kamera brauche, muss sie
141 Zugriff auf die Kamera haben.

142 A: Glaubst du, gibt es noch einen speziellen Grund, dass sie auf mehrere Bereiche zugreifen
143 möchte, die sie für keine Funktionen benötigt?

144 I: Nein.

145 A: Du hast gesagt, du machst auch Fotos mit deinem Smartphone.

146 I: Ja.

147 A: Angenommen du benützt dein Handy immer nur zu Hause und alleine, ohne, dass sich
148 jemand anderer neben dir oder im gleichen Raum aufhält. Denkst du, ist es dann dennoch
149 möglich, dass andere deine Fotos sehen können, ohne dass du sie ihnen zeigst oder schickst?

150 I: Wenn ich sie nur auf dem Handy hab, nein, schwierig.

151 A: Das heißt theoretisch wäre es möglich?

152 I: Sicher, theoretisch wäre es sicher irgendwie, ... nein, nein.

153 A: Ist es für dich realistisch, dass du anderen erlaubst deine Fotos anzusehen, ohne dass es dir
154 bewusst ist?

155 I: Nein, das glaube ich nicht. Obwohl, nein, denk ich nicht.

156 A: Wieso?

157 I: Nein. Nein. Wenn ich es nirgendwo verbunden habe.

158 A: Was heißt für dich verbunden?

159 I: Wenn ich das Handy mit dem Computer verbinde und die Fotos auf den Computer lade,
160 dann ist das schon möglich, aber, wenn ich es nie irgendwo verbinde, dann nicht.

161 A: Kann man das irgendwie kontrollieren, ob andere Personen oder Firmen Zugriff auf deine
162 Fotos haben?

163 I: Ja, das kann man sicher. Ja, nein, wenn sie dich hacken, dann hast du keinen Einfluss mehr,
164 aber sonst eigentlich schon.

165 A: Nehmen wir mal an, sie hacken dich nicht. Wie können andere legal Zugriff auf dein
166 Smartphone erhalten.

167 I: Ja, wenn ich ihnen das erlaube.

168 A: Wie erlaubst du ihnen das?

169 I: Wenn ich mich zum Beispiel verbinden würde oder so.
170 A: Glaubst du, dass das dann in deiner Hand liegt ob jemand auf dein Smartphone zugreifen
171 kann, oder glaubst du, dass du da gar nichts dagegen machen kannst? Größtenteils.
172 I: Nein, größtenteils liegt es sicher in meiner Hand.
173 A: Wie gut sind deine Fotos auf deinem Smartphone vor der Einsichtnahme anderer
174 geschützt?
175 I: Ja gut, denke ich.
176 A: Wer bestimmt die Sicherheit deiner Fotos auf deinem Smartphone?
177 I: Ja im Grunde ich selbst, vor allem.
178 A: Wenn du jetzt dein Smartphone benützt, kannst du ja auch alles zugreifen, auf Fotos,
179 Kalender, Alarm usw. Kannst du dir vorstellen, dass außer dir noch jemand Zugriff auf deine
180 Daten hat, oder nur du alleine?
181 I: Nur ich, wie gesagt, wenn ich es nicht verbinde, dann hat niemand Zugriff auf meine Daten.
182 Nein! Zugriff geht auch, weil mir ist es einmal passiert, dass ich den Wecker eingestellt habe
183 und er ist beim Marke 2 nicht abgegangen. Weil warum sollte er sonst nicht abgehen?
184 A: Das heißt?
185 I: Das heißt, du kannst es nicht selbst steuern.
186 A: Dann haben andere auch Zugriff oder was meinst du jetzt genau?
187 I: Ja, andere haben auch Zugriff, aber irgendwie sind sie verbunden.
188 A: Wer?
189 I: Die Firma, oder, ja die Firma.
190 A: Mit wem?
191 I: Mit dem Handy.
192 A: Und kannst du das aber unterbinden?
193 I: Nein.
194 A: Kannst du dir vorstellen, wie diese Firma den Zugriff erhält und wer ihnen das erlaubt?
195 I: Ja die Firma.
196 A: Aber die Firma ist ja die Firma, die Zugriff hat. Erlaubt sie sich selbst den Zugriff?
197 I: Ja das ist sicher in den Datenschutzrichtlinien drinnen, wenn sie, wenn irgendetwas ist, dass
198 das dann sein muss.
199 A: Somit erlaubst du das ihnen, eigentlich?
200 I: Ja, im Endeffekt erlaube ich es ihnen schon.
201 A: Wieso glaubst du braucht eine App Zugriff auf verschiedene Bereiche?

202 I: Das ist eine gute Frage. Ja sicher durch den Internetzugang, ... , warum sie auf den
203 Kalender? Nein, da hab ich keine Ahnung warum.

204 A: Was meinst du kann passieren, wenn die App Zugriff auf deine Fotos und Videokamera
205 hat, auf den Kalender, das Adressbuch. Was kann da sein?

206 I: Ja, dass sie dir Fotos nehmen, Adressbuch, die Adressen einfach rauskopieren, die
207 Nummern.

208 A: Und was machen sie dann mit den Nummern?

209 I: Ja, weiter verwenden oder ja.

210 A: Wie sieht das aus? Was machen sie dann?

211 I: Ja, wenn Nummern oder E-Mails drauf sind, dass sie die einfach anschreiben oder Werbung
212 machen. Dass sie immer wieder zu neuen Leuten auch kommen.

213 A: Gib es sonst auch noch einen Grund, dass diese Firmen diese verwenden?

214 I: [Pause]

215 A: Hast du schon mal davon gehört?

216 I: Ja, gehört schon, aber noch nie so richtig nachgedenkt.

217 A: Was nützen diesen Unternehmen eigentlich die Daten, wenn sie von dir das Adressbuch
218 haben, die Kalendernotizen.

219 I: Ja, da können sie Werbung machen, da können sie Umsatz machen. Ja, ich denk mir für das
220 sicher.

221 A: Vorwiegend einfach für Werbung?

222 I: Ja, oder ... eigentlich dürften sie das ja gar nicht.

223 A: Wieso nicht?

224 I: Ja eigentlich steht das wohl in den Datenschutzrichtlinien drinnen, dass sie die Daten nicht
225 nehmen von einem selbst. Müsste drinnen stehen, rechtlich gesehen, oder?

226 A: In der Datenschutzrichtlinie?

227 I: Ich unterschreibe ja, dass sie meine Daten verwenden dürfen, aber, dass sie ohne Erlaubnis
228 Daten von meinem Handy verwenden können, das steht sicher in einer Datenschutzrichtlinie
229 drinnen, dass sie das nicht dürfen.

230 A: Aber du liest die Datenschutzrichtlinie ja nicht immer durch, woher weißt du das?

231 I: Nein, nicht immer durch, aber das hört man immer.

232 A: Was hört man?

233 I: Dass sie das nicht dürfen. Einfach die Daten von deinem Handy nehmen, aber sie machen
234 das oft trotzdem. Das merkst du ja nicht mal, wenn sie sie nehmen oder nicht.

235 A: Kannst du das irgendwie überprüfen, ob jemand Daten von deinem Handy nimmt. Kann
236 man das irgendwo nachschauen?

237 I: Nein, ich wüsste das nicht. Ich wüsste nicht wo nachschauen.

238 A: Was glaubst du passiert, wenn eine Firma unzählig viele Daten von sehr, sehr vielen
239 Personen speichert?

240 I: Sie verwendet diese sicher weiter.

241 A: Und für was?

242 I: Ja ich denk mir Werbung, Umsatz sehen sie darin.

243 A: Kannst du dir auch noch etwas anderes vorstellen, was man mit den Daten machen kann?

244 I: [Schüttelt den Kopf].

245 A: Hast du dir schon mal überlegt Dienste oder Apps aufzugeben, weil sie den Zugriff auf
246 viele deiner Daten wollte?

247 I: Nein. Ich erlaube die Verbindung zum Internet nie und ansonsten akzeptiere ich sie nicht.

248 A: Was muss passieren, dass du eine App oder einen Dienst aufgibst und löschst?

249 I: Ja, wenn zum Beispiel ein Foto von mir als Werbung verwendet wird. Oder öffentlich oder
250 so.

251 A: Wie möchtest du dich in Zukunft vor der Datenspeicherung schützen?

252 I: Ja, indem ich den Apps die Verbindung zum Internet nicht erlaube. Aber die
253 Datenschutzrichtlinien sind einfach zu lang um sie zu lesen.

254 A: Wie denkst du wird unser Leben mit dem Smartphone in 30, 50 Jahren aussehen?

255 I: Ja, das wird noch schlechter enden als jetzt.

256 A: Was heißt schlechter enden?

257 I: Ja, sie reden immer von Datenschutzrichtlinien, im Endeffekt aber geschützt wird heute gar
258 nichts mehr. Und sie verwenden sie ja trotzdem. Und dass das einfach irgendwie ausartet,
259 dass jeder irgendwie zu Daten kommt, die er nicht einmal haben sollte oder haben dürfte.

260 A: Jetzt sag ich dir ein paar Szenarien und frag dich, ob diese für dich vorstellbar sind oder
261 nicht.

262 Wenn jemand täglich das Smartphone mit Apps und Internet zum Beispiel Twitter und/oder
263 Facebook nutzt, ohne jedoch jemals seinen Standort preiszugeben. Wäre es für dich dann
264 vorstellbar, dass man mit großer Wahrscheinlichkeit vorhersagen kann, wo sich derjenige in
265 Zukunft aufhalten wird?

266 I: Nein, das denke ich nicht.

267 A: Wieso?

268 I: Wenn er nie den Standort einschaltet, wie will dann jemand wissen, wo er ist?

269 A: Könntest du dir vorstellen, dass man zum Beispiel auch schon nur durch die Standorte von
270 ein paar Facebook-Freunden bestimmen kann, wo sich jemand aufhält?

271 I: Hm. Schwierig. Ja, wenn ich mich sonst immer mit denen aufhalte, vielleicht.

272 A: Hast du schon einmal davon gehört?

273 I: Nein, nicht im Speziellen.

274 A: Wie realistisch ist es für dich, dass die Polizei bereits heute wissen kann, wo morgen ein
275 Verbrechen stattfindet?

276 I: Wo morgen ein Verbrechen stattfindet? Hm, nein, unrealistisch.

277 A: Wieso?

278 I: Dann würden sie es wohl schon machen, wenn es das gäbe.

279 A: Nehmen wir mal an, dieses Verfahren wäre noch nicht erlaubt. Könnte es theoretisch
280 möglich sein?

281 I: Ma, möglich vielleicht schon.

282 A: Wie würde das funktionieren?

283 I: Das weiß ich nicht.

284 A: Hast du schon einmal davon gehört?

285 I: Nein.

286 A: Nehmen wir an, eine Frau kauft im Supermarkt verschiedene Sachen ein, jedoch keinerlei
287 Babysachen. Kannst du dir vorstellen, dass man nur aus den gekauften Artikeln mit hoher
288 Wahrscheinlichkeit sagen kann, ob diese Frau schwanger ist und ungefähr auch den
289 Geburtstermin feststellen kann?

290 I: Ja das vielleicht schon eher.

291 A: Wieso?

292 I: Ja, obwohl es gibt ja auch andere Leute, die sich gesund ernähren, und nicht schwanger
293 sind... hm. Nein, ich halte das für schwierig.

294 A: Was spricht dafür oder dagegen?

295 I: Ja, wenn sie schwanger ist, wird sie sich wohl gesund oder gesünder ernähren, würde ich
296 mal hoffen, aber nur das allein? Ich weiß nicht, es sind wohl andere Leute auch, die sich
297 gesund ernähren.

298 A: Hast du schon einmal davon gehört?

299 I: Nein.

300 A: Nehmen wir an, ein Mann ist homosexuell, er nützt das Internet, darunter auch Social
301 Media, gibt jedoch nirgends an, dass er Männer liebt. Sein Sexualleben wird also von ihm
302 nicht preisgegeben - weder im Internet, noch sonst irgendwo. Für wie realistisch hältst du es,

303 dass wildfremde Personen dennoch mit hoher Wahrscheinlichkeit sagen können, dass Max
304 homosexuell ist?

305 I: Ja, das halte ich schon für realistisch.

306 A: Wieso?

307 I: Ja, das sieht man einfach. Der braucht den nur mal zu beobachten. In seinem Verhalten
308 sieht er das sicher.

309 A: Wieso? Wie verhält sich ein Homosexueller?

310 I: Ja, das kann ich nicht so genau erklären, aber in manchen Situationen sieht man das einem
311 oft einfach an. Was soll ich sagen.

312 A: Hast du schon einmal davon gehört?

313 I: Nein, aber das sieht man ja selbst auch.

314 A: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft deine Freundesliste auf Facebook
315 kontrollieren und auch die Bewegungsdaten von deinem Smartphone heranziehen, wenn sie
316 prüfen wollen, ob du kreditwürdig bist oder nicht?

317 I: Ma, bei einer Kredit(...?) brauchst du nicht so viel, dass du überhaupt einen Kredit
318 bekommst.

319 A: Aber, wenn du jetzt sagst zum Beispiel beim Hausbauen oder für einen Autokauf?

320 I: Ja, da kannst du schon möglich sein. Sein sollte es zwar nicht, aber kann schon so kommen.

321 A: Wieso?

322 I: Ja, weil diese wollen sich ja auch absichern.

323 A: Kannst du dir das heute auch schon vorstellen?

324 I: Nein, heute noch nicht.

325 A: Kennst du die Gesundheits- und Fitnessapps, die man am Smartphone herunterladen kann?

326 I: Ja, kenn ich.

327 A: Kannst du dir vorstellen, dass in Zukunft Gesundheitsversicherungen prüfen, ob du
328 regelmäßig Sport machst und ob du dich gesund ernährst, wenn sie prüfen ob du eine
329 Versicherung bekommst oder welche?

330 I: Ja, das lass ich möglich sein.

331 A: Wieso?

332 I: Ja das ist wie bei den Kreditinstituten. Da geht es auch um viel Geld, die wollen sich halt
333 auch absichern.

334 A: Hast du schon einmal davon gehört?

335 I: Nicht direkt.

336 A: Wie wahrscheinlich hältst du die Vorstellung, dass man in Zukunft in ein Land nicht mehr
337 einreisen darf, weil man zum Beispiel ein bestimmtes Wort im Internet eingegeben hat?
338 I: Nein, das nicht. (lacht.) Das glaub ich nicht. Ein bestimmtes Wort wie meinst du das?
339 A: So ein Wort zum Beispiel, wie Amerika zerstören oder ein Wort, das Geheimdienste für
340 eine geheime Mission verwenden. Wenn du so ein Wort per SMS schreibst oder zum Beispiel
341 auf Google suchst, dass das für dich dann Folgen haben kann.
342 I: Eigentlich nicht.
343 A: Wieso nicht?
344 I: Das kann ich mir nicht vorstellen. Da müssten sie viel kontrollieren.
345 A: Du glaubst, es scheitert an den technischen Möglichkeiten?
346 I: Ja.
347 A: Hast du schon einmal davon gehört?
348 I: Nein.
349 A: Ist es für dich realistisch, dass man aus dem Verhalten der Vergangenheit, das Verhalten in
350 der Zukunft schon vorhersagen kann?
351 Ja, wenn er immer das gleiche nutzt und so oder immer das gleiche googelt, dann ist die
352 Wahrscheinlichkeit hoch, dass ihm das gefällt und dass er das dann auch macht.
353 A: Danke für das Interview.

1 **Interview 5, am 23.10.2014. Dauer 34:29 Minuten**

2

3 A: Wie alt bist du, und was machst du beruflich?

4 I: Also ich bin 24 und bin Beruf 5.

5 A: Mit welchen Medien informierst du dich vorwiegend?

6 I: Über das Internet.

7 A: Und wo schaust du da genau nach?

8 I: Also ich starte immer Google.

9 A: Aber auch so Zeitungen, oder Facebook?

10 I: Ach so, Nachrichten und so?

11 A: Ja, genau. Das Alltagsgeschehen und spezielle Nachrichten.

12 I: Da direkt Zeitungen.

13 A: Welche nutzt du da?

14 I: Ja vor allem den Spiegel und sonst Nachrichten in lokalen Medien, auch Fernsehen.

15 A: Radio?

16 I: Nein.

17 A: Social Media Seiten, wie Facebook oder so was?

18 I: Ja, Facebook bin ich dabei. Aber ich nutze es mehr so wie E-Mail.

19 A: So als Austauschplattform?

20 I: Ja, genau, so Messenger und so.

21 A: Täglich?

22 I: Ja, schon.

23 A: Welches Smartphone besitzt du?

24 I: Marke 1.

25 A: Für was gebrauchst du es?

26 I: Ich brauch es für Beruf 5 und vor allem auch, um im Internet nachzuschauen und die E-Mails zu
27 checken.

28 A: Telefonieren, SMS, Wecker?

29 I: Logisch, das auch.

30 A: Hast du auch Apps heruntergeladen?

31 I: Ja, hab ich.

32 A: Welche?

33 I: Ich habe die Onleihe, Onlinebibliothek, weil ich einfach das Gerät an den E-Reader
34 anschließe und dann über das Smartphone mir die Bücher aussuche, die ich mir dann

35 runterlade. Belletristik. Und sonst, was hab ich mir sonst noch runtergeladen? Gute Frage. Ja
36 ich geh meistens direkt in das Internet rein, das heißt ich lade mir nicht die Apps von den
37 Seiten herunter.

38 A: Ok, das heißt Facebook nützt du dann über das Internet?

39 I: Ja, genau, da bin ich schneller.

40 A: Taschenlampe oder so?

41 I: Taschenlampe hab ich jetzt!

42 A: Kalender- oder Wetter-App?

43 I: Kalender, ja Wetter-App. Die hab ich gleich auf der ersten Seite, die nehme ich nicht mal
44 mehr als App wahr.

45 A: Kalender oder Geburstagskalender?

46 I: Nein, Kalender nicht, da ist schon da, was automatisch oben war, der Gmail-Kalender. Da
47 sehe ich dann auch, wenn eine E-Mail kommt.

48 A: Spiele?

49 I: Spiele weniger. Ich hab schon ein Spiel drauf, also ich hab jetzt nicht vier, fünf Spiele
50 drauf, sondern ein Spiel, das ich manchmal am Abend verwende, um abzuschalten.

51 A: Ok, wie oft verwendest du die Apps, die du jetzt genannt hast?

52 I: Die Wetter, ok, die ist immer aktualisiert, sprich, ich schau drauf und nimm es nicht mal
53 wahr als App. Die Onleihe ja, weil ich einfach mir die Bücher rauflade und die Bücher dann
54 ja auch les.

55 A: Das heißt täglich oder fast jeden zweiten Tag?

56 I: Wenn ich dann das Buch fertiggelesen habe, sprich, für das Buch brauche ich zwei
57 Wochen, dann verwende ich es wieder.

58 A: Ok, das heißt immer im Rhythmus?

59 I: Genau. Und sonst gehe ich täglich ins Internet, also die Onlinezeitungen verwende ich
60 schon. Also ein Mal am Tag bin ich sicher drinnen.

61 A: Hast du schon einmal den Begriff Big Data gehört?

62 I: Nein.

63 A: Kannst du dir dennoch etwas darunter vorstellen?

64 I: Big Data, große Dateien? Aber ich weiß das jetzt nicht.

65 A: Hast du Datenschutz, ist dir das ein Begriff?

66 I: Ja, Datenschutz ist mir ein Begriff.

67 A: Wie gut kennst du dich mit Datenschutz aus?

68 I: Sagen wir so, man hat es auf der Uni ein bisschen gehört, was darf ich verwenden, was darf
69 ich nicht verwenden. Jetzt genau die Gesetze kenn ich nicht.

70 A: Erzähl mal: Was weißt du über Datenschutz? Oder wenn du jemandem erklären müsstest,
71 was Datenschutz ist.

72 I: Ok, wenn ich dir erklären müsste, was Datenschutz ist, dann würde ich einfach sagen,
73 welche Daten ich verwenden darf von anderen Leuten und welche Daten ich selbst reinstellen
74 darf.

75 A: Mhm. Ist das jetzt rein auf das bezogen, was du machen darfst, oder bezieht sich das auf
76 andere auch?

77 I: Ja, wie gesagt, jede eigene Person muss schauen, was darf ich reinstellen in das Internet und
78 was darf ich vom Internet verwenden. Das ist grob das, was globaler Datenschutz ist.

79 A: Ist das nur auf das Internet bezogen, oder gibt es das offline auch?

80 I: Nein, es ist offline. Und zwar, wenn ich zum Beispiel einen Film herunterlade. Das heißt
81 Filmdownload ist ja total verboten, weil auch wenn du es im Stream ansiehst, werden einfach
82 Teile heruntergeladen und diese sind dann auch im Offlinestatus auf deinem Computer drauf
83 und in diesem Moment bist du strafbar, wenn du diese Teile auf deinem Computer hast.
84 Natürlich Datenschutz kann in diesem Moment nicht klagen.

85 A: Aber im Grunde ist das dann immer in Verbindung mit dem Internet, oder?

86 I: Sagen wir so, es ist Datenschutz auch schon in der Bibliothek, als es Internet noch nicht
87 gab. Das heißt, wenn ein Lexika rausgekommen ist und ich hab das Wort für Wort
88 abgeschrieben, ohne zu verweisen, dass ich das von dem Lexika herausgeschrieben habe,
89 dann war auch dort schon immer Datenschutz im Spiel. Natürlich mit dem Internet ist das
90 jetzt mehr geworden.

91 A: Weil man leichter zu den Daten kommt?

92 I: Genau.

93 A: Hast du den Begriff Datenschutzrichtlinie, oder Datenschutzbestimmung schon mal
94 gehört?

95 I: Ja, aber frag mich nicht, was das ist.

96 A: Ok, dann frage ich: Was steht in einer solchen Datenschutzrichtlinie drinnen, zum
97 Beispiel?

98 I: Ich vermute es. Ich denke mir einfach, dass klar formuliert ist, was darf ich in einem
99 gewissen Bereich. Das heißt die Richtlinie zum Beispiel von den Fotos kann ich mir
100 vorstellen, wie viele Teile darf das Foto haben oder was muss geschwärzt werden. Wenn zum

101 Beispiel ich das Foto von einem Auto habe, muss das Nummernschild weg, ein schwarzer
102 Strich darüber.

103 A: Dass also die Persönlichkeit geschützt wird?

104 I: Ja.

105 A: Hast du bereits einmal eine Datenschutzrichtlinie durchgelesen?

106 I: Nein, ist glaub' ich langweilig.

107 A: Hast du einmal eine unterzeichnet oder unterschrieben?

108 I: Ja, und das startet schon, wenn man sich für Aktion 1 einschreibt. Das heißt man schreibt
109 schon dort, es passt, wenn ihr meine Fotos verwendet für eure Internetseite. Das heißt, das hat
110 sicher jeder. Auch schon in Ort 8 wird das gleich eingefordert am Anfang. Wenn sich jemand
111 einschreibt, wird eingefordert, was sie verwenden dürfen. Schon nur mal auf der Homepage
112 von Ort 8, darf dort Person 4 aufscheinen? Wenn ich im Internet suche Person 5, darf dann
113 aufscheinen, Person 5 ist in Ort 8?

114 A: Das heißt, du hast dir eine Richtlinie auch schon mal vollständig durchgelesen oder
115 überfliegst du sie nur?

116 I: Nein, ich überfliege diese Sachen. Nein, aber die, die ich unterschrieben habe waren immer
117 kurz, das heißt, diese hab ich dann immer auch gelesen.

118 A: Wenn wir nun an deine Apps denken: Haben diese überhaupt Datenschutzrichtlinien?

119 I: Ja, immer am Anfang, wenn man sie installiert glaub ich, dann kommt, was sie verwenden
120 von mir.

121 A: Hast du dir diese mal durchgelesen oder angesehen?

122 I: Ich schau mir immer an, was sie von mir verwenden. Das heißt, wenn sie wirklich sagen ich
123 verwende zum Beispiel, ich hab das nicht kombiniert, zum Beispiel die Kreditkarte, das
124 kommt ab und zu, ich hab das nicht kombiniert, das heißt mein Smartphone kennt meine
125 Kreditkarte nicht. Und das heißt bei solchen Apps passe ich auf und les mir das genauer
126 durch.

127 A: Auf was greifen deine Apps dann so zu?

128 I: Meistens ist Foto dabei.

129 A: Deine Fotodateien oder Fotokamera?

130 I: Fotodateien ist meistens auch dabei bei den Apps. Meistens lad ich sie hoch und lösche sie
131 dann wieder, weil ich mir denke, die brauch ich sowieso nicht. Ein paar hab ich schon wieder
132 gelöscht. Das heißt, ja Foto war oft dabei und was war dann sonst noch dabei? An diese
133 erinnere ich mich noch, weil das Symbol da ist, und eben an Kreditkarte kann ich mich
134 erinnern, weil ich geschockt war, wieso sie die Kreditkarte brauchen.

135 A: Welche Datenschutzrichtlinien haben deine Apps? Weißt du was darüber?
136 I: Nein, nicht genau.
137 A: Wo kann man sich über diese Datenschutzrichtlinie z.B. von Apps informieren?
138 I: Ich würde mal sagen beim Verbraucherschutz.
139 A: Gibt's auch eine Möglichkeit, sich bei der App direkt zu informieren?
140 I: Ich denke mal im Internet, wenn du suchst diese App und Datenschutz, dann findest du
141 sicher was. Also da bin ich ganz zuversichtlich, dass man da was findet.
142 A: Du hast gesagt, die App möchte auf Fotos zugreifen oder auf die Kreditkarte. Wieso
143 meinst du braucht die App Zugriff auf verschiedene Bereiche?
144 I: Es ist oft denke ich, dass die App sagt ok, dass, um zu funktionieren braucht es oft
145 verschiedene, weil zum Beispiel oft braucht man ein Profilfoto oder so. Deshalb sagen sie,
146 Foto, will ich zugreifen können, weil sonst, wenn man das nicht von vornherein sagt, dann ist
147 das ein Problem. Wenn man in der App drinnen ist, dann kann man nicht mehr diesen Link
148 machen.
149 A: Ok. Dann müsste man das immer extra raupladen?
150 I: Mhm.
151 A: Und wer erlaubt ihnen dann den Zugriff eigentlich?
152 I: Den hab ich ihnen erlaubt.
153 A: Könntest du dir vorstellen zum Beispiel, dass die Wetter-App sagt, um funktionieren zu
154 können, brauche ich Zugriff auf deine Kamera?
155 I: Nein.
156 A: Und Zugriff auf dein Adressbuch zum Beispiel oder deine E-Mailkontakte zum Beispiel?
157 I: Könnte ich mir so nicht vorstellen. Sie fragt zum Beispiel immer den Ort ab, das heißt, den
158 Standort will sie wissen. Das ist auch immer etwas was immer nachgefragt wird. Und den
159 Standort sag ich zum Beispiel, dass er automatisch nicht preisgegeben wird, das heißt ich
160 gebe den Standort nicht an, das mag ich nicht. Und ich kann mir schon vorstellen, dass die
161 Wetter-App startet und sagt immer das Wetter an, wo ich gerade bin. Beim Titelbild kommt
162 dann immer das Wetter, wo ich gerade bin. Wenn ich in Ort1 bin, kommt das Wetter von
163 Ort1, wenn ich in Ort2 bin, dann von Ort2.
164 A: Aber sie hat dann Zugriff auf deinen Standort oder nicht?
165 I: Nein, bei mir nicht, ich hab ihr das verweigert. Sie sagt mir immer nur von Ort1 an.
166 A: Gibt es einen speziellen Grund, wieso du ihr das verweigerst?
167 I: Ich sage, je weniger man erlaubt, umso besser ist das. Weil irgendwann weiß das Internet
168 mehr über dich, als du über dich selbst.

169 A: Hast du das Gefühl so, oder hast du das mal irgendwo gelesen?
170 I: Nein, das ist ein bisschen durch das Studium bedingt. Studium 3.
171 A: Also ist das schon Absicht, dass du deine Daten nicht freigibst.
172 I: Ja.
173 A: Wieso meinst du, verlangen manche Apps Zugriff auf Bereiche, welche sie für keine
174 Funktion benötigen?
175 I: Ja damit sie an mehr Daten kommen.
176 A: Ok. Nutzt du dein Smartphone auch um Fotos zu machen?
177 I: Ja.
178 A: Angenommen, die Anna benützt ihr Handy immer nur zu Hause und alleine, ohne, dass
179 sich jemand anderer neben ihr oder im gleichen Raum aufhält. Denkst du, ist es dann dennoch
180 möglich, dass andere ihre Fotos sehen können, ohne dass sie es ihnen zeigt oder schickt?
181 I: Wenn sie immer nur offline ist, dann nicht, aber wenn sie ein einziges Mal online ist, dann
182 schon.
183 A: Wieso?
184 I: Weil in dem Moment, wenn du online bist, gibt es Menschen, die besser sind beim
185 Computer, als du selbst. Und diese können alles machen.
186 A: Und diese Personen stehlen dann die Fotos?
187 I: Du kommst einfach in jeden Computer rein, in dem Moment, wenn du online bist, können
188 andere Personen rein.
189 A: Unerlaubt?
190 I: Unerlaubt.
191 A: Könntest du dir zum Beispiel auch vorstellen, dass die Anna erlaubt, dass ihre Fotos
192 weitergegeben werden, ohne, dass es ihr bewusst ist?
193 I: Ja, das geht zu schnell. Eben, wenn man sagt zu einer App, du darfst das verwenden, in dem
194 Moment kommt das einfach rein.
195 A: Wie gut sind deine Fotos jetzt auf deinem Smartphone geschützt?
196 I: Meine Fotos, erstens habe ich nicht so viele Fotos drauf, und diese Fotos geb ich dann auf
197 den Computer. Aber auch beim Computer ist es das gleiche. In dem Moment, wenn ich online
198 bin, kommen die Personen an meine Fotos. Ich sage immer, man muss auch, ich hab keine
199 Fotos, die jemand nicht sehen darf. Und ich denke mir, so startet es. Du schützt dich selbst,
200 indem du nur gewisse Fotos von dir machst.
201 A: Wer bestimmt die Sicherheit deiner Fotos auf deinem Smartphone?

202 I: Ich selbst, aber das hat man einfach nicht mehr unter Kontrolle. In dem Moment, wenn du
203 online bist.

204 A: Und wie kannst du diese Sicherheit kontrollieren oder bestimmen?

205 I: Die Sicherheit ist sicher einmal, wenn ich sage, ich verkaufe meine Geräte, das ist ein Teil
206 der Sicherheit, den du sicher mitmachen kannst. Das heißt, das gesamte Gerät formatieren.
207 Ich weiß, auch wenn du deine Geräte formatierst, da sind immer Teile noch drauf und diese
208 bekommen sie auch. Das ist einmal der erste Schutz. Also nicht nur löschen und dann
209 verkaufen. Das ist ein Schutz, den ich selbst machen kann. Wie du es noch schützen kannst?

210 Ja, durch eine externe Platte, das heißt ich habe meine Bilder nicht auf dem Computer,
211 sondern auf der externen Platte und lade sie dann immer runter. Ich habe dann immer nur
212 mehr Teile auf dem Computer und nicht mehr das Ganze und da sage ich dann, dass es
213 einfach schwerer ist, darauf zuzugreifen.

214 A: Ist es auch möglich zu kontrollieren, wer jetzt genau Zugriff hat auf deine Fotos oder
215 nicht? Oder zu kontrollieren ob auch Fotos zum Beispiel von deinem Smartphone
216 runtergeladen werden von Apps, die gar nicht danach fragen? Kann man das irgendwo
217 kontrollieren oder sehen?

218 I: Also ein paar Sachen kann man schon sperren, aber ich sage, du sperrst das dann für die
219 Normalsterblichen. Wenn jemand gut beim Computer ist, dann ist jedes Sperren umsonst.

220 A: Ok. Wenn wir nun an dein Smartphone im Speziellen denken, kannst du das kontrollieren
221 oder überprüfen am Smartphone selbst?

222 I: Ja bei den Einstellungen selbst kann man das überprüfen.

223 A: Was können Apps machen, die deine Fotos haben, dein Adressbuch, diese gesamten
224 Informationen?

225 I: Also das Adressbuch dient sicher dazu, die Daten weiterzugeben, mit den Fotos fehlt mir
226 meine Phantasie, um zu wissen, was die mit meinen Fotos anfangen könnten.

227 A: Ok, aber im Grunde speichern diese die Daten irgendwo mal, oder?

228 I: Mhm.

229 A: Wer könnte daran interessiert sein, deine Fotos zu speichern?

230 I: Das... Ich denke Fotos haben für andere keinen Wert. Fotos haben für mich einen eigenen
231 Wert, das ist gleich wie ich nicht die Fotos von jemand anderem haben möchte. Aber ich
232 denke, da muss man in die Köpfe der anderen Leute rein denken.

233 A: Was können Unternehmen zum Beispiel machen, wenn sie nicht nur deine Daten haben,
234 sondern von unzählig vielen Personen den Standort, die Fotos usw.?

235 I: Das ist sicher mal eine Kontrolle, das heißt, für was sie die Kontrolle dann verwenden, das
236 ist sicher ein (Lebens?) zum Beispiel, die Idee ist, welche einige Leute haben vom Internet
237 her, auch vom Einkaufen her, sage ich weiß deinen Geschmack, den sehe ich ja auf den Fotos,
238 dann kann ich dir ja die Werbung so schicken, dass du meine Sachen kaufst.

239 A: Also steht Verkauf und Werbung dahinter?

240 I: Mhm.

241 A: Ok. Welche Folgen kann das für uns noch haben?

242 I: Es ist sicher auch im Gesetz, abgesehen davon, dass Datendiebstahl gesetzlich nicht erlaubt
243 ist, aber ich denke mir einfach, man weiß einfach nicht, was in den Köpfen der Leute vorgeht.
244 Wenn jemand beginnt, jemandem nachzuspionieren aus irgendeinem Grund, dann ist das
245 nicht angenehm, wenn er meine Fotos hat und mir dann diese Fotos womöglich mit der Post
246 schickt.

247 A: Ok, ganz die schlimme Variante. Hast du dir schon überlegt, einen Dienst oder eine App
248 aufzugeben, weil du gedacht hast, der bekommt zu viele Informationen von mir?

249 I: Nein, das noch nie. Ich hab einige abgelehnt, weil mir die Liste zu lang war. Ach ja, wo
250 ganz viele Informationen gesammelt werden, ist zum Beispiel Dropbox. Das hab ich auch auf
251 dem Smartphone, weil da hab ich auch überlegt.

252 A: Was war der Grund, dass du es dann behalten bzw. installiert hast?

253 I: Weil ich hab für meine Tante schauen wollen, wie es funktioniert, weil ich selbst es nicht
254 kannte. Und es ist halt fein. Logisch auf die Fotos muss es zugreifen, weil sonst bekommst du
255 die Fotos nicht hoch. Und du kannst dann auf Distanz, oder auf der Uni haben es bei uns viele
256 verwendet, um am gleichen Projekt zusammenzuarbeiten.

257 A: Praktisch mur, aus Kosten-Nutzen- Gründen. Der Nutzen, den du daraus gezogen war, hast
258 höher als die Kosten?

259 I: Ja.

260 A: Kennst du noch jemanden, der einen Dienst aufgegeben hat, weil er oder sie gesagt hat, die
261 Datenspeicherung war zu groß?

262 I: Nein, aber darüber wurde auch nicht geredet.

263 A: Was müsste für dich zum Beispiel passieren, dass du sagst, du gibst Facebook oder so
264 einen Dienst zum Beispiel wirklich auf?

265 I: Also Facebook zum Beispiel, ok, das habe ich extrem gesperrt, ich habe dort auch alle
266 Fotos gelöscht, weil ich sage, wenn die Person 4 reinkommen würden, das möchte ich nicht.
267 Alle jetzt auch nicht, aber sagen wir so, die Fotos wo ich in Ort3 zum Beispiel beim
268 Ausgehen war, habe ich gelöscht. Und da ist wirklich, wenn ich höre, da kursieren ein paar

269 Geschichten die Runde in Ort 8, was auf Facebook oder so gegangen ist, dann raus damit und
270 weg. Wenn ich sehe, da gibt es ein Loch. Weil in Ort 8 ist es einfach kritisch mit den
271 Personen 4.

272 A: Das heißt Geschichten über dich?

273 I: Ja. Wenn sie zum Beispiel meine Kommunikationen wissen würden. Das merkst du dann
274 auch, ob sie das gelesen haben. Wenn sowas passieren würde, dann wäre ich draußen.

275 A: Wenn deine Privatsphäre nicht mehr geschützt wäre?

276 I: Ja.

277 A: Wie möchtest du dich in Zukunft vor dem schützen?

278 I: Ja, das gibt es ja schon bei den Apps. Das kann man schon bei den Einstellungen machen.
279 Da muss man dann sich auch die Mühe machen die Einstellungen zu suchen und dann das
280 Häkchen bei Privacy, Privacy, Privacy zu machen.

281 A: Wie denkst du wird unser Leben mit der Technologie und mit dem Smartphone in 30, 50
282 Jahren aussehen?

283 I: Da kann alles sein. Da können auch gar keine mehr da sein.

284 A: Wer kann nicht mehr da sein?

285 I: Gar keine Smartphones etc. mehr. Komplett was neues. Aber steigern oder so, dass die
286 Leute noch mehr Handys und Tablets haben, das denke ich nicht. Ich denke wir sind schon
287 auf einem Höhepunkt angekommen, weil ein Handy rechts, ein Handy links, mehr hat in der
288 Hosentasche nicht mehr Platz.

289 A: Aber wie denkst du, wird sich das mit den Daten entwickeln?

290 I: Das mit den Daten wird immer sensibler, aber der Datenschutz greift meistens dort an, wo
291 man ihn nicht braucht, und wo es absurd ist.

292 A: Das heißt jetzt?

293 I: Dort, wo es wirklich lästig ist. Zum Beispiel [zum Schutz der Anonymität wird dieser
294 persönliche Teil des Interviews nicht transkribiert].

295 A: Ich verstehe. Gut, jetzt schildere ich dir ein paar Szenarien und frage dich ob du diese für
296 realistisch hältst oder nicht.

297 Wenn jemand täglich das Smartphone mit Apps und Internet zum Beispiel Twitter und/oder
298 Facebook nutzt, ohne jedoch jemals seinen Standort preiszugeben. Wäre es für dich dann
299 vorstellbar, dass man mit großer Wahrscheinlichkeit vorhersagen kann, wo sich derjenige in
300 Zukunft aufhalten wird?

301 I: Ja.

302 A: Wieso?

303 I: Das ist machbar. Weil eigentlich in dem Moment wo das Handy sucht, jedes Mal, wenn ich
304 eigentlich Empfang habe, nicht im Flugmodus bin, schickt mein Handy ja immer Suchmodus
305 zum Masten aus und somit in dem Moment wo ich den Masten suche, geht das auch in die
306 andere Richtung.

307 A: Gut, ja. Könntest du dir aber auch vorstellen, wenn wir sagen, derjenige verliert sein
308 Handy und ist somit nicht mehr erreichbar für andere, kann man dann dennoch irgendwie
309 herausfinden, wo sich derjenige aufhalten wird?

310 I: Also den letzten Standort vom Handy sicher und dann natürlich mit der Zeit, sieht man ja
311 wie er sich vorher bewegt hat, mit welcher Geschwindigkeit, ob er zu Fuß unterwegs war.
312 Logisch nachher kann man dann hypothetische Kreise ziehen. Wenn er mit dem Auto
313 unterwegs war, dann ist er in diesem Radius, hat er einen (?), dann ist das dieser Radius, ist er
314 vielleicht in der Nähe eines Flughafens, ok Flugzeug, ok, dann in einer Stunde ist er in einem
315 weiteren Radius zu suchen.

316 A: Ok. Kannst dir auch vorstellen, dass wenn man sich da zum Beispiel mit Freunden, wenn
317 man Facebookfreunde hat, dass man sich schon nur durch ein paar Freunde den Standort
318 ungefähr ausrechnen kann, auch wenn man von der Person X, sage ich mal, keine
319 Informationen hat?

320 I: Ah, wenn man nur die Informationen von den Freunden hat?

321 A: Ja, zum Beispiel.

322 I: Ok, dann sicher. Weil, wenn jetzt ein Freund den Standort preisgibt, dann musst du den
323 wohl kennengelernt haben. Es gibt dann schon Personen, die nur hypothetische Freunde
324 haben auf Facebook, dann natürlich weniger, aber dann merkst du das auch, weil er wird sich
325 nicht alle hypothetischen Freunde aus Ort1 suchen.

326 A: Also kann man das dann schon relativ genau festlegen.

327 I: Mhm, ja.

328 A: Hast du schon einmal davon gehört?

329 I: Von?

330 A: Dass das möglich ist?

331 I: Nein, das kann ich mir zusammenrechnen, als Studentin 3.

332 A: Wie realistisch ist es für dich, dass die Polizei bereits heute wissen kann, wo morgen ein
333 Verbrechen stattfindet?

334 I: In dem Moment, wenn sie die Daten kontrollieren, aber dann bewegen sie sich auch nicht
335 auf legalem Boden.

336 A: Welche Daten?

337 I: Wenn sie einfach Gespräche abhören, oder einfach, wenn sie sehen jetzt kommuniziert
338 dieser mit jenem oder wenn wir bei Facebook bleiben, jetzt hat der mit dem Freundschaft
339 geschlossen und sagen wir mal ein Verbrecher ist aus Ort 2 und er hat jetzt mit einem
340 Verbrecher aus Ort 3 Freundschaft geschlossen, dann machen die gemeinsame Sache
341 entweder oben oder unten. Oder auf dem Weg.

342 A: Ok, nehmen wir mal an, es ist nicht eine spezielle Person, die sie kontrollieren, wo die das
343 Verbrechen plant, sondern wirklich die Polizei geht her und schaut, wo in Ort 2 ist in den
344 nächsten 48 Stunden ein Verbrechen? Ohne, dass sie eine spezielle Person oder Personen
345 untersuchen.

346 I: Ok, dann würde ich schauen, wo finden die Partys statt.

347 A: Wieso die Partys?

348 I: Nein, wie gesagt Treffen. Einfach, wenn sie lesen Studentenparty, dann schaut einer Mal
349 vorbei, oder wenn es einen Termin für Essensausgabe der Obdachlosen gibt und sie wissen,
350 dass immer zwei, drei in eine Prügelei verwickelt sind, dann fährt eine Streife dort hin.

351 A: Ok, das heißt im Grunde, sie suchen nach Zusammenhängen sozusagen?

352 I: Ja, genau. Wo es schon mal war, wird es eher wieder vorkommen.

353 A: Hast du schon einmal davon gehört?

354 I: Nein, wenn, dann unterbewusst.

355 A: Nächstes Beispiel: Nehmen wir an, eine Frau kauft im Supermarkt verschiedene Sachen
356 ein, jedoch keinerlei Babysachen. Kannst du dir vorstellen, dass man nur aus den gekauften
357 Artikeln mit hoher Wahrscheinlichkeit sagen kann, ob diese Frau schwanger ist oder nicht
358 und ungefähr auch in welchem Monat?

359 I: Ja, vielleicht ein paar Ernährungsberater sicher.

360 A: Wieso? Wieso Ernährungsberater.

361 I: Man sieht das schon, wenn man sagt, da ist die Schwangerschaftsgruppe jedes Mal und zum
362 Beispiel ein Doktor, der immer sagt, ok, in der dritten Woche esst mehr Karotten und macht
363 das in Kombination mit zwei Tomaten jeden Tag, dann spiegelt sich das einfach wieder. Ich
364 denk, jetzt nur von dem, wenn man sagt ok, ich bin Ernährungsberater und schau mir das jetzt
365 in Deutschland an, wenn man die Gewohnheiten des Doktors nicht kennt und was er den
366 Schwangeren sagt, ist es nicht möglich.

367 A: Ok, aber wenn man eigentlich ein bisschen weiß, was Frauen in der Schwangerschaft so
368 einkaufen an Lebensmitteln und anderen Sachen, dann kann man sich das ausrechnen?

369 I: Genau.

370 A: Wie funktioniert das dann?

371 I: Einfach aus dem, ja das ist einfach Kaufverhalten. Aber das, du darfst das jetzt nicht sagen
372 heute, ok logisch, wenn du jetzt zwei Mal diese Frau beobachtest, dann ist es logischer, weil
373 sonst kannst du immer sagen ok, das ist Zufall heute, die hat heute halt Hunger auf Karotten
374 und so.

375 A: Ok. Hast du schon einmal davon gehört?

376 I: Ha. Nein, das vom Kaufverhalten schon, das sieht man einfach im Fernsehen, aber jetzt
377 direkt, dass man auf Schwangere schließt nicht.

378 A: Ok, aber das Kaufverhalten.

379 I: Ja.

380 A: Nehmen wir an, ein Mann ist homosexuell, er nützt das Internet, darunter auch Social
381 Media, gibt jedoch nirgends an, dass er Männer liebt. Sein Sexualleben wird also von ihm
382 nicht preisgegeben - weder im Internet, noch sonst irgendwo. Für wie realistisch hältst du es,
383 dass wildfremde Personen dennoch mit hoher Wahrscheinlichkeit sagen können, dass der
384 Mann homosexuell ist?

385 I: Wenn er homosexuelle Freunde hat.

386 A: Wieso ist das dann für ihn auch zutreffend?

387 I: Weil in dem Moment, was du bist, in diesem Freundeskreis bewegst du dich.

388 A: Hast du schon einmal davon gehört?

389 I: Nein, ich habe viele homosexuelle Freunde. Kennst du einen, lernst du alle kennen.

390 A: Also im Grunde über andere dann?

391 I: Ja, weil am Anfang kannte ich keinen, dann habe ich einen kennengelernt, dann habe ich
392 alle gekannt.

393 A: Ok. Kannst du dir auch vorstellen, dass man es rausfinden kann zum Beispiel indem man
394 kontrolliert ob dieser, jetzt zum Beispiel, wenn alle homosexuellen Männer einen gelben
395 Pullover haben und man kontrolliert ob er auch einen gelben Pullover hat, dann ist die
396 Wahrscheinlichkeit schon ein bisschen größer.

397 I: Ja.

398 A: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft deine Freundesliste auf Facebook
399 kontrollieren und auch die Bewegungsdaten und so, wenn sie prüfen wollen, ob du
400 kreditwürdig bist oder nicht?

401 I: Ja.

402 A: Wieso?

403 I: Das wird schon gemacht.

404 A: Ah, das wird schon gemacht? Weißt du das oder hast du schon einmal davon gehört?

405 I: Nein, das ist immer, das ist automatisch, das ist auch wenn du auf Arbeitssuche gehst, das
406 gleiche machen die Banken halt auch. In dem Moment, wenn ich Arbeit suche, was macht
407 mein Chef? Gibt im Internet meinen Namen ein. Und je nachdem was er findet, ist dann halt
408 ja oder nein.

409 A: Ok.

410 I: Ja logisch es ist immer so, wenn es um eine Entscheidung geht. Weil wenn ich der einzige
411 auf dem Markt bin, der diese Arbeit machen kann, dann wird er sich diesen Weg mit dem
412 Internet sparen, weil er sagt, ok das will ich nicht wissen. Aber in dem Moment, wenn zwei
413 Leute diese Arbeit möchten, dann ist das halt ein Auswahlverfahren. Kann Vorteile und
414 Nachteile mitbringen. Sagen wir so, ich bin bei einem Verein und dem anderen gefällt das,
415 dem anderen kann es nicht gefallen.

416 A: Und mit dem Kredit kannst du dir das auch vorstellen, dass sie dich kontrollieren?

417 I: Logisch, weil in dem Moment, wenn du bei einer Bank einen Kredit anfragst, wird dir die
418 Bank nie gleich am ersten Tag sagen ok, ich gebe ihn dir, sondern was macht sie? Sie sagt
419 immer, ich frage nach, komm morgen wieder. Das hört man nie, dass sie einen Kredit gleich
420 gibt. Was machen sie an diesem Tag? Sie checken dich durch von oben bis unten.

421 A: Gut. Kennst du die Gesundheits- und Fitnessapp's, die man am Smartphone herunterladen
422 kann?

423 I: Ja, ich werde diese sicher nie verwenden.

424 A: Wieso nicht?

425 I: Ich finde, die verstärken das alles und dann wirst du einfach extrem.

426 A: Ok, aber nicht aus Datenschutzgründen?

427 I: Nein, nicht aus Datenschutzgründen.

428 A: Kannst du dir vorstellen, dass in Zukunft Gesundheitsversicherungen sich mit solchen
429 Apps zusammenschließen und dann wirklich kontrollieren, ob du regelmäßig Sport machst
430 und ob du dich gesund ernährst, wenn sie prüfen welche Versicherung du bekommst oder ob
431 du überhaupt eine Versicherung bekommst?

432 I: Mhm.

433 A: Wieso?

434 I: Ja, dann sparen sie sich die Arbeit im Internet. Dann bekommen sie die Daten direkt.

435 A: Das heißt? Was heißt das dann?

436 I: In dem Moment, wenn du eine Versicherung abschließt, ist das gleich wie bei einem Kredit,
437 die checken dich durch.

438 A: Mhm, ok.

439 I: Und in dem Moment, wenn sie wissen ok, der ist bei dieser App, dann haben sie das gratis
440 und mit weniger Aufwand.

441 A: Hast du schon einmal davon gehört?

442 I: Nein. Ich habe das halt von den Banken gehört, bei den Arbeitsgebern weiß man es und
443 dann ist es logisch, dass das andere auch machen.

444 A: Ok, dann kombinierst du die Informationen.

445 I: Ja.

446 A: Wie wahrscheinlich hältst du das Szenario, dass man in Zukunft in ein Land nicht mehr
447 einreisen darf, weil man zum Beispiel ein bestimmtes Wort im Internet eingegeben hat oder
448 per SMS oder E-Mail etwas schreibt?

449 I: Jetzt momentan denke ich, ist es noch ziemlich liberal, aber logisch, wenn ein Land
450 umschlägt und extrem wird, derzeit ist es so, du darfst in ein paar Länder gar nicht einreisen,
451 wenn du den falschen Stempel im Reisepass hast. Wenn du einen Stempel vom Irak drinnen
452 hast, darfst du gar nicht mehr in die USA einreisen. Dann musst du einen neuen Pass machen.

453 A: Kannst du dir vorstellen, wenn jemand einem Kollegen in einer SMS schreibt: Wir werden
454 uns in der USA zerstören, dass derjenige Probleme bekommt beim Einreisen, dass sie ihn
455 vielleicht gar nicht einreisen lassen zum Beispiel?

456 I: Ja, kann ich mir sehr gut vorstellen. Momentan, hoffe ich, ist es noch nicht so.

457 A: Wieso? Wie funktioniert das?

458 I: Spionage. (lacht).

459 A: Hast du schon einmal davon gehört?

460 I: Nein, es ist halt, ja eigentlich letztes Jahr war das ja immer in den Medien mit der Spionage
461 und Deutschland, ich will das nicht, und hin und her.

462 A: NSA?

463 I: Ja, wo Politiker extra andere Handys bekommen haben, mit denen sie nicht mehr abgehört
464 werden konnten und dann ist das normal irgendwie. Weil wieso spioniert man jemanden
465 nach? Um irgendwann Sanktionen zu setzen.

466 A: Ok, das letzte Beispiel:

467 I: Ist es für dich realistisch, dass man aus dem Verhalten der Vergangenheit, das Verhalten in
468 der Zukunft schon vorhersagen kann?

469 A: Ja, bei vielen. Aber ich würde es mir nie zumuten, weil ich sage, jemand kann sich auch
470 ändern.

471 I: Mhm. Aber wieso ist das grundsätzlich möglich?

472 A: Du kannst heute deinen Charakter nicht komplett verändern. Deshalb, was du mal gemacht
473 hast, man sagt ja, der Täter kehrt immer zum Tatort zurück.

474 I: Also, wenn wir jetzt ganz normale Personen annehmen, wie du und ich, könnte man das
475 dann auch schon sagen?

476 A: Ja, wenn dir nie Knödel geschmeckt haben, werden sie dir auch in Zukunft nicht
477 schmecken. Dann wäre es unsinnig dir Knödelwerbung zu schicken.

478 A: Ja gut, das war's. Danke für das Interview.

1 **Interview 6, am 24.10.2014. Dauer 26:27 Minuten**

2

3 A: Wie alt bist du, und was machst du beruflich?

4 I: Ich bin 22, beruflich bin ich Beruf 2.

5 A: Mit welchen Medien informierst du dich vorwiegend?

6 I: Für was genau?

7 A: Für alltägliche Sachen.

8 I: Ja mit dem Internet.

9 A: Und wo genau?

10 I: Wo genau? Über welche Informationen?

11 A: Ja, zum Beispiel Nachrichten oder auch spezielle Themen.

12 I: Also Nachrichten schau ich bei WhatsApp, Facebook, Google.

13 A: Hast du zum Beispiel auch stol, oder Spiegel oder so was?

14 I: [Interviewpartner schweift ab]. Nein.

15 A: Zeitungen?

16 I: Nein, les ich auch nicht.

17 A: Radio, hörst du das manchmal?

18 I: Nein.

19 A: Schaust du im Fernsehen manchmal Nachrichten oder so?

20 I: Ich habe keinen Fernseher.

21 A: Hast du auf Facebook? Zum Beispiel, ich habe Spiegel Online geliked und bekomme jetzt
22 immer wieder neue Postings.

23 I: Nein, Nachrichten deprimieren.

24 A: Ah, dann versuchst du sie zu meiden?

25 I: Ja, da steht immer nur Negatives drinnen.

26 A: Ja, meistens. Gut. Welches Smartphone besitzt du?

27 I: Marke 2 Model 6, glaube ich.

28 A: Für was gebrauchst du es?

29 I: Für Höraudios hören, für Musik, SMS schreiben, im Internet sein, telefonieren, Arbeit, Wecker.

30 A: Hast du auch Apps auf dein Smartphone heruntergeladen?

31 I: Ja, das für Musik. Sonst eigentlich keine. WhatsApp.

32 A: Was ist das welche MusikApp?

33 I: [Erklärt die App].

34 A: Hast du sonst so WetterApp?

35 I: [Schüttelt verneinend den Kopf]
36 A: Geburtstagskalender oder sowas?
37 I: [Schüttelt verneinend den Kopf]
38 A: Taschenlampe?
39 I: Taschenlampe habe ich. Aber die brauche ich fast nie.
40 A: Hast du dir die als App runtergeladen?
41 I: Nein, die war schon drauf. Ah! Ich hab doch eine App. Ein Foto-Dings-Da.
42 A: Instagram?
43 I: Nein. Da kannst du verschiedene Farben und Einstellungen vornehmen und Fotos
44 bearbeiten. YouTube hab ich noch.
45 A: Wie oft verwendest du diese Apps?
46 I: Eigentlich immer.
47 A: Jeden Tag?
48 I: Ja das mit den Fotos nicht, aber Facebook, und WhatsApp und das mit der Musik auch.
49 A: Hast du schon einmal den Begriff Big Data gehört?
50 I: Nein.
51 A: Kannst du dir dennoch etwas darunter vorstellen?
52 I: Datenschutz denke ich mal.
53 A: Begriff Datenschutz: Ist dir das bekannt?
54 I: Neein, nicht genau.
55 A: Aber generell?
56 I: Ja, dass man Daten nicht weitergeben darf.
57 A: Ok. Wie gut kennst du dich mit Datenschutz aus?
58 I: Gar nicht.
59 A: Wenn du jemandem erklären müsstest was Datenschutz ist, was würdest du dann sagen?
60 I: Dann würde ich sagen, dass deine Daten geschützt werden und nicht weitergegeben werden
61 an Dritte.
62 A: Hast du schon mal den Begriff Datenschutzrichtlinie, oder Datenschutzbestimmung
63 gehört?
64 I: Mhm.
65 A: Was steht in einer solchen Datenschutzrichtlinie drinnen?
66 I: Boha, keine Ahnung! Dass es nicht an Dritte weitergegeben wird. Aber das weiß ich nicht.
67 A: Aber das kannst du dir vorstellen, dass das drinnen steht?
68 I: Ja, sicher.

69 A: Nutzerbestimmung oder Nutzerbedingungen, hast du das schon einmal gehört?
70 I: Ja, das hab ich auch schon mal gehört.
71 A: Ist das dir ein Begriff, oder weißt du genau was das ist?
72 I: Keine Ahnung, was das ist.
73 A: Hast du bereits einmal eine Datenschutzrichtlinie unterzeichnet?
74 I: Ja sicher, das bei WhatsApp steht das ganz unten drunter, gel? Bei Facebook auch. Bei den
75 Online-Dings-Da.
76 A: Hast du das nur Online gemacht, oder hast du außerhalb des Internets auch schon mal eine
77 Datenschutzrichtlinie unterschrieben?
78 I: Bei Firma 1, sonst glaub ich, in der Schule muss man das auch machen. Beim Handy!
79 A: Wenn wir nun an deine Apps denken: Meinst du, dass deine Apps Datenschutzrichtlinien
80 haben?
81 I: Keine Ahnung, ja die normalen üblichen schon, aber die „extra“-Apps, so wie diese Foto-
82 Dings, sicher nicht.
83 A: Mit den normalen meinst du Facebook und WhatsApp und so?
84 I: Ja, die normalen werden das schon haben.
85 A: Hast du dir schon mal eine durchgelesen?
86 I: Nicht wirklich, die sind immer so lang.
87 A: Welche Datenschutzrichtlinien haben deine Apps?
88 I: Keine Ahnung.
89 A: Wo kann man sich über solche Datenschutzrichtlinie informieren z.B. von Apps?
90 I: Im Internet.
91 A: Wo dort?
92 I: Ja da brauch man nur in Google reinschreiben Datenschutz, irgendwo.
93 A: Meinst du bei den Apps selbst auch?
94 I: Ja, das steht sicher irgendwo. Ganz unten glaub ich steht das immer, dass man das auch
95 nochmal nachlesen kann, oder so.
96 A: Ok. Auf welche Daten von dir können Apps zugreifen? Nehmen wir mal als Beispiel
97 Facebook oder WhatsApp. Auf was können diese Apps zugreifen auf deinem Handy?
98 I: Auf die Telefonnummer, glaube ich.
99 A: Nur auf deine?
100 I: Nein, die verbindet sich dann glaub ich automatisch, dass das Profil dann auf meinem
101 Handy angezeigt wird, weißt du, von anderen Leuten.

102 A: Ok, das heißt, das Profil, das du und andere online haben geht automatisch auf dein
103 Handy?
104 I: Mhm.
105 A: Haben sie Zugriff auf dein Adressbuch jetzt zum Beispiel auch?
106 I: Ma, das weiß ich nicht.
107 A: Ok, sonst was, worauf sie zugreifen können? Fotos oder so?
108 I: Ja, die Fotos, die ich poste schon, aber die anderen nicht, oder?
109 A: Ich weiß nicht.
110 I: Ja, ich auch nicht! Ja keine Ahnung!
111 A: Aber Fotos kannst du dir vorstellen, dass die, die du postest, dass sie Zugriff haben?
112 I: Ja, auf die haben sie dann Zugriff. Jaja, weil da ist mal gestanden, wenn man das nicht
113 erlaubt, dann kann man das auch nicht posten. Du musst zuerst das aktivieren, dass das
114 erlaubt wird.
115 A: Wie sieht es mit dem Standort aus, zum Beispiel?
116 I: Ah ja, das ist auch, dass man das aktivieren muss.
117 A: Hast du das aktiviert?
118 I: Nein, hab ich mal gehabt, hab es dann aber wieder entfernt. Muss nicht jeder wissen, wo ich
119 überall bin und wem ich schreibe.
120 A: Internetzugriff, meinst du, das haben sie auch?
121 I: Ah, dass drinnen steht, dass ich online bin, oder so?
122 A: Nein, dass die praktisch, wenn du Facebook auf deinem Handy hast, dass sie dann
123 zugreifen können. Dass du praktisch in das Internet reingehen kannst über Facebook App oder
124 WhatsApp.
125 I: Das geht ja automatisch oder geht das gar nicht?
126 A: Ja, aber sie müssen ja einen Zugriff haben, weil wenn du zum Beispiel ihnen das nicht
127 erlaubst oder das Internet ausschaltest, weil du zum Beispiel dafür extra bezahlen müsstest,
128 I: Dann geht es doch?
129 A: Nein, dann geht es nicht, weil sie brauchen halt den Zugriff, so gemeint.
130 I: Ah, so!
131 A: Gut, du hast gesagt, du nutzt dein Smartphone auch, um Fotos zu machen. Jetzt schildere
132 ich dir ein Szenario:
133 Angenommen, die Anna benützt ihr Handy immer nur zu Hause und alleine, ohne, dass sich
134 jemand anderer neben ihr oder im gleichen Raum aufhält und sie hat eben auch Fotos auf

135 ihrem Handy. Denkst du, ist es dann dennoch möglich, dass andere ihre Fotos sehen können,
136 obwohl sie Fotos nie weitergibt oder schickt?

137 I: Hm, ja die Hacker oder so vielleicht schon.

138 A: Mhm, und diese hacken sich in ihr Handy?

139 I: Ja sicher, diese Leute gibt es immer.

140 A: Und könntest du dir vorstellen, dass sie eigentlich anderen Leuten erlaubt, ihre Fotos
141 anzusehen, aber ihr ist es nicht wirklich bewusst?

142 I: Durch die Dings, wo man immer ok drückt?

143 A: Was sind diese Dings?

144 I: Ja, die Datenschutz. Steht das da drinnen?

145 A: Theoretisch zum Beispiel, ja.

146 I: Muss ich mir doch mal durchlesen, aber das ist so lang immer, da steht unmöglich viel
147 drinnen.

148 A: Kannst du dir vorstellen, dass da im Datenschutz was drinnen steht, dass sie Zugriff auf die
149 Fotos haben und man drückt halt ok, weil man es sich nicht durchliest und somit haben andere
150 Leute eigentlich Zugriff auf die Fotos, aber einem selbst ist das nicht bewusst.

151 I: Ja sicher. Ja, es gibt so viele Sachen.

152 A: Wie gut sind deine Fotos auf deinem Smartphone vor der Einsichtnahme anderer
153 geschützt?

154 I: Puh, wenn ich mir das nie durchgelesen habe, dann weiß ich nicht, ob das nicht irgendwo
155 mal dabei war.

156 A: Was glaubst du?

157 I: Nein, ich denke nicht, dass das wer anderer sieht. Hoffen wir mal.

158 A: Ok. Wer bestimmt die Sicherheit deiner Fotos auf deinem Smartphone?

159 I: Ich selbst. Nein ich weiß nicht. Ja, ich selbst logisch, ich muss selbst schauen.

160 A: Und wie kannst du das sehen wer Zugriff hat oder nicht? Oder kannst du das überhaupt
161 kontrollieren, deine Sicherheit? Gibt es das überhaupt, dass du das kontrollieren kannst oder
162 bist du da ausgesetzt?

163 I: Das sind Fragen. Ich weiß nicht, sollte ich mal nachschauen bei diesen Datenschutz-Dings.

164 A: Ok, da könntest du es kontrollieren?

165 I: Ja, denke ich mir.

166 [...]

167 A: Wer, außer dir hat noch alles Zugriff auf deine Fotos, deine Kalendernotizen, dein
168 Adressbuch usw.?

169 I: Hm. Andere Leute. Ich weiß nicht.
170 A: Irgendwelche Apps auch? Wo du denkst, das könnte eigentlich schon sein, dass diese
171 Zugriff hat?
172 I: Ja, WhatsApp. Ja immer die gleichen zwei. Sind immer nur die.
173 A: Facebook und WhatsApp?
174 I: Mhm.
175 A: Auf welche Bereiche haben diese Apps jetzt genau Zugriff?
176 I: Ja Fotos, Telefonnummern und die ganzen Sachen.
177 A: Was ist noch bei den ganzen Sachen dabei?
178 I: Ja, Fotos und Telefonnummern und die Adressen, die du drinnen gespeichert hast.
179 A: Sonst auf noch irgendwas außer diese zwei Sachen?
180 I: (...?) Nein.
181 A: Den Zugriff erhalten sie, hast du gesagt, durch die Datenschutzrichtlinien, ok?
182 I: Mhm.
183 A: Wieso meinst du, brauchen Facebook und WhatsApp Zugriff auf deine Fotos und dein
184 Adressbuch?
185 I: Bo, weil sie das sammeln und dass sie einfach wissen, wer zu wem gehört und irgendwie
186 keine Ahnung, dass das irgendwie alles vernetzt ist.
187 A: Mhm. Was nutzt ihnen das, wenn sie wissen, wer zu wem gehört und wie das
188 zusammengestellt ist?
189 I: Hm. Bo, ich glaube ich hab mal gehört, dass man diese Daten auch verkaufen kann, dass
190 man da auch so Handel machen kann. Ich weiß nicht, dann bekommst auch Werbungen
191 zugeschickt, von diesen Sachen.
192 A: Ja, wo hast du davon gehört? Weißt du das noch? In Nachrichten oder von anderen
193 Leuten?
194 I: Keine Ahnung, Allgemeinwissen, nein. (lacht).
195 A: Welche Daten brauchen Apps von dir, um funktionieren zu können?
196 I: Ich denke den Namen, die E-Mailadresse und vielleicht, dass sie manchmal die
197 Telefonnummer brauchen, kann das sein?
198 A: Jetzt sag ich dir ein Beispiel: Nehmen wir mal an, eine deiner Foto-App sagt sie braucht
199 Zugriff auf das Internet, um funktionieren zu können. Denkst du das braucht sie wirklich, um
200 funktionieren zu können?
201 I: Ja, sonst wird es nicht gehen.

202 A: Und wie sieht es aus, wenn sie sagt, sie braucht Zugriff auf dein Adressbuch, damit sie
203 funktionieren kann? Denkst du dir dann, ja doch, kann schon sein, sonst kann sie nicht
204 funktionieren?

205 I: Bei WhatsApp vielleicht schon, Facebook vielleicht nicht.

206 A: Und wenn wir an deine Foto-App denken, wenn diese sagt, ich brauche Zugriff auf dein
207 Adressbuch, sonst kann ich nicht funktionieren.

208 I: Nein, das ist unlogisch. Wenn sie sagt, sie braucht Zugriff auf deine Fotos, das ist dann
209 schon eher logisch.

210 A: Was ist, wenn sie sagt, sie braucht Zugriff auf deinen Kalender, sonst kann sie nicht
211 funktionieren?

212 I: Nein, glaub ich nicht.

213 A: Wieso meinst du, sagt eine solche App, dass sie Zugriff auf das Internet, auf das
214 Adressbuch und Fotos usw. braucht, obwohl sie rein von der Funktion her den Zugriff auf
215 diese Bereiche gar nicht brauchen würde?

216 I: Weil da jemand dahinter ist, der die Daten will.

217 A: Ja, und mit diesen Daten macht er dann wieder das gleiche?

218 I: Sich alles zusammenstellen, ja.

219 A: Gut, wieso werden diese Daten gespeichert?

220 I: Damit man alles zurückverfolgen kann.

221 A: Mhm. Kontrolle?

222 I: Ja. Bo, sonst geht es vielleicht auch um die Sicherheit.

223 A: Für dich selbst jetzt oder für andere Leute vielleicht, oder für beides?

224 I: Bo, allgemein eigentlich. Für andere Leute auch zum Beispiel. Es gibt ja nicht ganz ehrliche
225 Leute, dass keine Ahnung, die Polizei da ein bisschen schauen kann.

226 A: Kannst du diese Speicherung auch irgendwie verhindern oder beeinflussen oder so?

227 I: Welche Speicherung?

228 A: Von deinen Daten jetzt zum Beispiel. Also wenn die App deine Adressbuchdaten zum
229 Beispiel speichert.

230 I: Was kann ich machen?

231 A: Kannst du das verhindern?

232 I: Wenn ich Nein anklicke. Blockieren oder so.

233 A: Ok, gut. Wenn wir denken, ein Unternehmen erstellt eine App. Was kann das
234 Unternehmen machen, wenn sie nicht nur von dir sämtliche Daten haben, wie Adressbuch,
235 Fotos, Notizen, Kalender usw., sondern von unzählig vielen anderen Person auch unzählig

236 viele Daten haben. Du hast gesagt die machen dann so ein Schema mit den vielen Kontakten,
237 wer wen kennt und so. Gibt es noch einen Grund, wofür ihnen das nützt? Oder was sie da
238 herausfinden können?

239 I: Nein, keine Ahnung. Bei Dings-Da weiß ich halt, wenn du verschiedene Sachen eingibst
240 bei Google oder Facebook, dann kommen genau diese Werbungen, wofür du dich interessiert
241 hast.

242 A: Ok, dass sie dich dann genau ansprechen können?

243 I: Ja, ganz genau.

244 A: Was kann das für uns welche Folgen haben, wenn über uns alle Daten offen sind?

245 I: Keine Ahnung. Ich weiß nicht, was da welche Nachteile sind.

246 A: Hast du dir schon überlegt, einen Dienst oder eine App deswegen aufzugeben, weil diese
247 so viele Daten von dir nimmt?

248 I: Das merkt man nicht, ob diese so viele Daten nimmt.

249 A: Kannst du das sehen, oder kontrollieren, wer oder wie viele Daten eine App nimmt?

250 I: Nein, das kann man nicht.

251 A: Aber könntest du dir vorstellen, dass wenn du rausfindest, dieser Dienst nimmt sehr viele
252 Daten von mir, dass du diesen dann beendest, weil du sagst, das möchte ich nicht?

253 I: Eigentlich, ich weiß jetzt nicht, welchen Nachteil das hat, wenn jemand die Daten hat über
254 einen anderen.

255 A: Aber auch, wenn du jetzt nicht weißt, welche Nachteile das haben könnte, rein vom Gefühl
256 her, dass du sagst, nein ich möchte eigentlich gar nicht, dass derjenige alles über mich weiß,
257 auch wenn ich nicht genau weiß, was der andere jetzt anstellt mit diesen Daten, ist das für
258 dich ein Punkt, wo du sagst, nein das möchte ich gar nicht? Oder was müsste passieren, dass
259 du sagst, diese Foto-App lösche ich, weil?

260 I: Über das habe ich überhaupt nie nachgedacht.

261 A: Ok, hast du dir schon Gedanken gemacht, oder machst du dir jetzt gerade Gedanken, wie
262 du dich in Zukunft vor dieser Datenspeicherung schützen kannst?

263 I: Ich werde mir nachher dann deine Tipps anhören.

264 A: Ok, das ist ein guter Vorschlag.

265 Wie denkst du wird unser Leben mit dem Smartphone in 30, 50 Jahren aussehen?

266 I: Ja, noch viel extremer. Noch viel mehr online und so.

267 A: Das heißt dann kann man auf Daten leichter zugreifen?

268 I: Ja, sicher.

269 A: Ok. Ich werde dir nun ein paar Szenarien schildern und dich fragen, ob du diese für
270 realistisch hältst oder nicht.

271 Wenn jemand täglich das Smartphone mit Apps und Internet zum Beispiel Facebook oder
272 auch Twitter aber niemals seinen Standort preisgibt. Wäre es für dich dann vorstellbar, dass
273 man mit großer Wahrscheinlichkeit vorhersagen kann, wo sich derjenige in Zukunft aufhalten
274 wird?

275 I: Ja.

276 A: Wieso?

277 I: Das wissen diese Leute immer, ich weiß nicht. Weil weißt du, das kann man sicher
278 irgendwie orten oder so. Weil das Handy kannst du ja auch, wenn du es verlierst, kannst du es
279 ja auch orten und so.

280 A: Kannst du dir auch vorstellen, dass das nicht mal unbedingt mit dieser Person selbst etwas
281 zu tun hat? Dass, wenn man zum Beispiel Freunde auf Facebook hernimmt und diese
282 Standorte heranzieht, dass es dann irgendwie möglich ist, den Standort von dieser Person X
283 ausrechnen kann, obwohl sie ihren Standort nicht angibt und praktisch unsichtbar ist?

284 I: Ja sicher. Wenn die anderen zum Beispiel Fotos reinstellen, dann kommt man sicher
285 irgendwie drauf, wo diese andere Person ist.

286 A: Ja, kannst du dir auch vorstellen, dass man nur durch die Standortdaten der Facebook-
287 Freunde in diesem Fall den Standort der anderen Person ermitteln kann?

288 I: Ja, irgendwie ist das sicher möglich.

289 A: Kannst du dir auch erklären wie ungefähr?

290 I: Nein.

291 A: Hast du davon auch schon mal gehört?

292 I: Ja, das hört man schon öfters.

293 A: Ah schon?

294 I: Ja man hört irgendwie, dass jeder weiß, wo du irgendwie bist, irgendwie durch diese Apps
295 oder durch Facebook oder so.

296 A: Wo hast du das gehört?

297 I: Ma, keine Ahnung. Von anderen Personen.

298 A: Wie realistisch ist es für dich, dass die Polizei bereits heute wissen kann, wo morgen ein
299 Verbrechen stattfindet?

300 I: Ja, wenn sie gut sind und das irgendwie durch die Medien, aber sie werden nicht so blöd
301 sein und das über WhatsApp ausmachen. Nein, das ist unrealistisch.

302 A: Kannst du dir vorstellen, dass man das durch so Statistiken irgendwie herausfinden kann,
303 dass man sieht, wenn heute hier ein Verbrechen ist, dann kann morgen dort eines sein,
304 übermorgen da eines.

305 I: Nein, nicht realistisch.

306 A: Wieso nicht?

307 I: Weil hier bei uns fast nie ein Verbrechen ist.

308 A: Wenn du jetzt an größere Städte, wie London, New York, oder so denkst?

309 I: Wenn es dort öfters passiert, vielleicht schon. Ist es realistischer, aber hier bei uns.

310 A: Also kommt es auf die Häufigkeit von den Verbrechen drauf an, oder auf was kommt es
311 drauf an?

312 I: Ja, wenn man ein Schema herausarbeiten kann.

313 A: Hast du schon einmal davon gehört, dass das möglich ist?

314 I: Ja, wenn sie einen abhören. Zum Beispiel am Handy. Das ist ja auch oft, dass sie einen
315 abhören und wenn du dann zum Beispiel gewisse Wörter sagst und so. Da hören sie dir ja
316 auch zu. Das hab ich in der Schule gelernt.

317 A: Super, mal was Nützliches. Wenn sie jetzt aber nicht speziell auf Personen achten, wer ein
318 Verbrechen plant, sondern wirklich nur wo. Also auch nicht Informationen heranziehen, wer
319 was plant, sondern mehr Informationen heranziehen, welche Verbrechen früher passiert sind.

320 I: Nein, dann ist es unrealistisch.

321 A: Dann, das dritte Beispiel: Nehmen wir an eine Frau kauft im Supermarkt verschiedene
322 Sachen ein, jedoch keinerlei Babysachen. Kannst du dir vorstellen, dass man nur aus den
323 gekauften Artikeln mit hoher Wahrscheinlichkeit sagen kann, ob diese Frau schwanger ist
324 oder nicht und in welchem Monat sie ungefähr ist?

325 I: Ehrlich, gibt es das? Nein, das ist unrealistisch.

326 A: Wieso nicht?

327 I: Zahlt sie in bar oder mit Kreditkarte?

328 A: In bar.

329 I: Nein, das ist unrealistisch.

330 A: Wieso?

331 I: Ja, keine Ahnung. Weil du heute viele Sachen einkaufst, dann kannst du nicht. Überhaupt
332 mit bar sieht ja niemand was sie einkauft, sondern nur mit Kreditkarte, kannst du alles
333 nachverfolgen und auch mit der Steuernummer. Da wäre es eher realistisch.

334 A: Wieso dann eher?

335 I: Weil es dann irgendwo gespeichert wird. Weißt du, wenn du in bar zahlst, dann scheint es
336 nirgendwo auf, dass du das bezahlt hast. Und wenn du mit Kreditkarte zahlst oder deine
337 Steuernummer angeben musst, dann wird es irgendwo registriert.

338 A: Also praktisch, wenn sie schon wissen, dass diese Frau schwanger ist, dann schließen sie
339 auf das zurück? Weil, wenn andere das nicht wissen und mit Kreditkarte bezahlen, was wäre
340 dann?

341 I: Nein, das mit dem Schwanger sein, das wissen sie nicht. Nein, unrealistisch.

342 A: Hast du schon einmal davon gehört?

343 I: Nein.

344 A: Nehmen wir an, ein Mann ist homosexuell, er nützt das Internet, darunter auch Social
345 Media, darunter Facebook und solche Sachen, gibt jedoch nirgends an, dass er Männer liebt
346 und er hält sein Sexualleben auch geheim und gibt es weder im Internet, noch sonst irgendwo
347 an. Für wie realistisch hältst du es, dass eine wildfremde Person dennoch mit hoher
348 Wahrscheinlichkeit sagen kann, dass der Mann homosexuell ist oder?

349 I: Ja, wenn er sich kleidet, wie einer.

350 A: Ja, wieso dann?

351 I: Ja, bei manchen Personen sieht man das beim Gewand, wie sie mit den Händen tun, wie sie
352 reden und von der Stimme.

353 A: Kannst du dir auch vorstellen, dass man das dann über das Internet herausfinden kann,
354 ohne dass man den Mann sieht? Live vor sich hat?

355 I: Ja. Wieso soll das dann nicht funktionieren?

356 A: Ok, dass er dann in diesen Punkten mit anderen Homosexuellen übereinstimmt?

357 I: Ja.

358 A: Hast du schon einmal davon gehört?

359 I: Ja.

360 A: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft deine Freundesliste auf Facebook
361 kontrollieren und auch die Bewegungsdaten von deinem Smartphone heranziehen, wenn sie
362 prüfen wollen, ob du kreditwürdig bist oder nicht und welchen Kredit du bekommst?

363 I: Ja, das denke ich mir schon, dass sie das beginnen. Das machen ja auch schon die
364 Arbeitgeber, wenn sie jemanden anstellen, schauen sie zuerst auf Facebook.

365 A: Wieso hältst du das für realistisch?

366 I: Weil sie mehr Sicherheit haben möchten, dass der Kredit wieder zurückkommt, oder halt
367 das Geld.

368 A: Hast du schon einmal davon gehört?

369 I: Nein.

370 A: Kennst du diese Gesundheits- und Fitnessapp's, die man am Smartphone herunterladen
371 kann, wo man eingibt, was man isst oder wie viel man trainiert?

372 I: Ja.

373 A: Kannst du dir vorstellen, dass in Zukunft Gesundheitsversicherungen sich mit solchen
374 Apps zusammenschließen und wirklich überprüfen, ob du dich ausreichend bewegst und was
375 du isst, wenn sie prüfen, welche Gesundheitsversicherung sie dir anbieten?

376 I: Hm. Ja, könnte möglich sein.

377 A: Wieso?

378 I: Nein, du fragst Fragen! Ja, damit sie dann genauer schauen können. Keine Ahnung.

379 A: Damit es für sie sicherer wird?

380 I: Ja, damit sie auch wissen, wie die Leute sind und wie sie sich ernähren.

381 A: Hast du schon einmal davon gehört?

382 I: Nein.

383 A: Wie wahrscheinlich hältst du das Szenario, dass man in Zukunft in ein Land nicht mehr
384 einreisen darf, weil man zum Beispiel ein bestimmtes Wort im Internet eingegeben hat?

385 I: Ja, möglich ist das schon, aber dann müssten sie ja alles überprüfen.

386 A: Ja. Kannst du dir das also vorstellen?

387 I: Ja, schwierig. Hm. Jeden anschauen müssten sie dann ja.

388 A: Hälts du das technisch für nicht machbar?

389 I: Ich weiß nicht.

390 A: Hast du schon einmal davon gehört?

391 I: Ja, man weiß ja zum Beispiel, dass man in Amerika sehr stark kontrolliert wird, wenn man
392 einreist. Es könnte schon möglich sein, aber ich glaube, dass da der Aufwand zu groß ist.

393 A: Ist es für dich realistisch, dass man aus dem Verhalten der Vergangenheit, das Verhalten in
394 der Zukunft schon vorhersagen kann?

395 I: Ja eigentlich schon, aber ein Mensch ändert sich ja immer ein wenig.

396 A: Aber du kannst dir vorstellen, dass, wenn man sagt, der war früher so, dass es dann
397 wahrscheinlich ist, dass er in Zukunft so oder so ähnlich sein wird.

398 I: Ja, das schon, halt immer nur mit einer gewissen Wahrscheinlichkeit.

399 A: Gut, das war's. Danke für das Interview.

1 **Interview 7, am 25.10.2014. Dauer 32:31 Minuten**

2

3 A: Wie alt bist du, und was machst du beruflich?

4 I: 24 und arbeite als Beruf 2.

5 A: Mit welchen Medien informierst du dich vorwiegend über allgemeine Sachen?

6 I: Bücher und Internet.

7 A: Welche vorwiegend?

8 I: Also ich nutze sicher das Internet und auch Bücher lese ich täglich, also.

9 A: Was suchst du im Internet?

10 I: Wenn ich Infos brauch, schnell mal ein Wort übersetzen in eine andere Sprache, danehm
11 ich nicht mehr das Lexikon wie damals, den Duden besser gesagt, sondern das geht mit
12 Internet schneller.

13 A: Hast du auch so Zeitungen, die du online liest?

14 I: Nein.

15 A: Liest du Zeitungen generell, liest du das? So Zeitungen, Tageszeitungen, Wochenmagazine
16 oder sonst was?

17 I: Es kann passieren, wenn ich in der Zeitung blättere, in der Zeitung 1 oder in der
18 Tageszeitung. Aber selten.

19 A: Hast du vielleicht auf Facebook so Zeitungen, wie Stol zum Beispiel, die immer wieder
20 Informationen posten?

21 I: Nein, also das interessiert mich nicht viel.

22 A: Radio?

23 I: Höchstens beim Autofahren.

24 A: Fernsehen?

25 I: Wenig Zeit für Fernsehen, und wenn, dann einmal einen Film am Samstag- oder
26 Sonntagabend.

27 A: Gut, welches Smartphone besitzt du?

28 I: Marke 1.

29 A: Für was gebrauchst du dein Smartphone?

30 I: Privat und beruflich.

31 A: Und was machst du alles damit?

32 I: Was ich alles mache? Ich telefoniere, ich schreibe SMS, WhatsApp logisch ganz viel und Internet.

33 A: Wecker.

34 I: Auch.

35 A: Hast du auch Apps heruntergeladen?

36 I: Also WhatsApp, Facebook, was hab ich dann noch heruntergeladen? YouTube, dann eines
37 für tägliche Sprüche, positive Gedanken am Tag, Wecker-App, soll ich kurz schauen?

38 A: Ja, kannst du gerne. Wetter?

39 I: Wetter? Nein.

40 A: Taschenlampe?

41 I: Ja, Taschenlampe, das hab ich oben, dann eine Sport-App.

42 A: Was hast du welche Sport-App? So Informationen über bestimmte Sportergebnisse oder
43 generell was für einen Sport, den du jetzt machst?

44 I: Zehn Minuten Videos.

45 A: So Motivations- oder Trainingsvideos.

46 I: Trainingsvideos! Zehn-Minuten-Übungen.

47 A: Ok.

48 I: Die habe ich, dann habe ich ein Veganes-App mit Rezepten, dann Skype, Viber, und eine
49 App von Robin (...?).

50 A: Mhm, hast du auch so Kalender, oder ist das schon drauf, so Geburtstagskalender?

51 I: Es ist ein Kalender von Marke 1 schon drauf, aber den nutze ich nicht für Geburtstage.

52 A: Wie oft verwendest du diese Apps.

53 I: Manche gar nie. Also ich bin nicht so der App-Typ. Ich nehme mir das, was ich brauche,
54 wie WhatsApp, Facebook oder E-Mail, diese Sachen, oder zwei drei Apps beruflich. Das ist
55 eigentlich das, was ich hauptsächlich nutze.

56 A: Hast du schon einmal den Begriff Big Data gehört?

57 I: Nein.

58 A: Kannst du dir dennoch vorstellen, was man darunter versteht?

59 I: Big Data?

60 A: Ja.

61 I: Also ich hoffe es hat jetzt nichts mit einer Date-App zu tun?

62 A: Ach so, nein.

63 I: Nein, ich weiß es nicht.

64 A: Hast du, Datenschutz ist dir das ein Begriff?

65 I: Ja.

66 A: Wie gut kennst du dich mit Datenschutz aus?

67 I: Nicht gut.

68 A: Wenn du jemandem erklären müsstest, was Datenschutz ist, was würdest du dann sagen?

69 I: Also Datenschutz würde ich vom Wort hernehmen, dass meine Daten geschützt sind.
70 A: Mhm.
71 I: Aber was in der heutigen Zeit nicht mehr so der Fall sein wird.
72 A: Hast du den Begriff Datenschutzrichtlinie, oder Datenschutzbestimmung schon mal
73 gehört?
74 I: Ja.
75 A: Weißt du auch, was in einer solchen Datenschutzrichtlinie drinnen stehen könnte?
76 I: Nein.
77 A: Hast du bereits einmal eine Datenschutzrichtlinie unterschrieben? Oder zugestimmt?
78 I: Online meinst du?
79 A: Online, oder offline.
80 I: Meinst du bei Verträgen, dort auch?
81 A: Mh, zum Beispiel.
82 I: Ja, ich glaube schon. Für die Privacy, ist das das gleiche?
83 A: Ja, das kann sich überschneiden.
84 I: Sind das Gesetze, oder?
85 A: Ja, das sind so Richtlinien, wie deine Daten geschützt werden.
86 Weißt du zufällig, wo du mal so eine Richtlinie unterzeichnet hast?
87 I: Bei Firma1 habe ich das unterschrieben, soweit ich weiß.
88 A: Haben deine Apps auch Datenschutzrichtlinien, oder eigene Datenschutzrichtlinien?
89 I: Ich glaube nicht. Nein, ich glaube nicht.
90 A: Wenn du eine App herunterladest, musst du dann
91 etwas zustimmen oder erlauben am Anfang?
92 I: Ja, akzeptieren.
93 A: Hast du dir das mal durchgelesen?
94 I: Ob ich lese, was da steht? Nein.
95 A: Was meinst du akzeptierst du da, bei diesem Text, den du nicht liest. Was könnte da
96 drinnen stehen?
97 I: Sind das die AGB's.
98 A: Unter anderem kann es auch das sein, das kann alles da dabei sein, ja.
99 Nutzungsbestimmung heißen sie das zum Beispiel auch.
100 I: Ja, ok. Die Sachen auch vom Datenschutz, dass sie die Sachen verwenden können, die ich
101 rauflade. Wie zum Beispiel bei Facebook ist mir schon passiert, dass mein Profilbild, das war
102 in der Ort4-Zeitung drinnen. Und da haben sie einen Artikel gehabt über Facebook , ob wir

103 wissen, was mit den Sachen die wir reinstellen eigentlich getan werden kann. Und da haben
104 sie mein Foto drinnen gehabt. Dann hab ich mir gedacht: Ok.

105 A: Bist du erschrocken, oder?

106 I: Ich hab mich gefragt, ob sie das machen dürfen? Aber sie dürfen das machen, weil alles was
107 ich reinstelle, dürfen sie hernehmen. Auch bei WhatsApp.

108 A: Ok. Das, was du praktisch zustimmst beim Akzeptieren, ist im Grunde so ein, kann einmal
109 die Datenschutzrichtlinie sein, es kann auch eine Nutzungsbestimmung sein, wo Datenschutz
110 aber immer mit drinnen ist, wo du praktisch akzeptierst, dass sie deine Daten verwenden
111 dürfen.

112 Wo meinst du kann man sich über die Datenschutzrichtlinien jetzt zum Beispiel von den Apps
113 informieren?

114 I: Bei der App selbst.

115 A: Und wo dort?

116 I: Ja, wenn man es runterladest, dann bekommt man das immer zum Lesen, aber wenn du es
117 verneinst, dann bekommst du sie ja gar nicht, oder einmal. Und dann vielleicht bei der App
118 selbst gibt es sicher irgendwas, wo man nachschauen kann. Wenn man sich genauer mit der
119 App beschäftigt. Aber ich bin mir jetzt auch nicht sicher.

120 A: Aber du glaubst schon, dass es bei der App was gibt?

121 I: Ja.

122 A: Auf welche Daten meinst du können deine Apps jetzt von deinem Smartphone zugreifen?

123 I: Nochmal?

124 A: Wenn du Apps runterladest auf dein Smartphone, auf welche Daten, die du auf dem
125 Smartphone gespeichert hast, können deine Apps zugreifen?

126 I: Meine Apps, meine Daten [sehr erschrocken]. Das hoff ich wohl nicht, dass meine Apps auf
127 meine Daten zugreifen können.

128 A: Nehmen wir mal an, Facebook zum Beispiel, wenn du ein Bild auf Facebook rauploadest,
129 hat es dann Zugriff auf deine Fotos?

130 I: Die auf meinem Handy oben sind?

131 A: Ja.

132 I: Nein. [mit erschrockenem Unterton].

133 A: Wie sieht es mit WhatsApp aus? Hat WhatsApp Zugriff auf deine Kontakte, auf dein
134 Adressbuch, praktisch auf die Nummern?

135 I: Nein. Gmail ist glaub ich so ein Kandidat, oder Google.

136 A: Gmail hast du auch, hast du gesagt?

137 I: Ja.
138 A: Auf was hat das dann Zugriff?
139 I: Die glaub ich auf alles.
140 A: Was fällt unter alles?
141 I: Nein, wenn du es synchronisierst oder so, es hat ja immer auch, wenn du eine E-Mail
142 schreibst, dann findest du die im Telefonbuch wieder, die E-Mail.
143 A: Die Adresse?
144 I: Ja. Und die wär ja wahrscheinlich nicht im Telefonbuch, wenn Gmail oder Google, ich
145 weiß nicht wer in diesem Fall das ist, da nicht Zugriff hätte.
146 A: Synchronisiert, meinst du da mit dem Handy synchronisiert oder mit dem Computer?
147 I: Mit meinem Handy.
148 A: Mit deinem Handy. Ok. Hat dann Gmail auch Zugriff auf deine Fotos, weil du gesagt hast
149 die haben auf alles Zugriff. Fallen da Fotos und Kalender und so auch rein?
150 I: Fotos da muss man was zustimmen, dass die Fotos synchronisiert werden mit, keine
151 Ahnung, Google, irgendwas.
152 A: Ok.
153 I: Dass, wenn man das Handy verliert, dann die Fotos noch hätt.
154 A: Ja, genau. Machst du auch Fotos mit deinem Smartphone?
155 Jetzt sag ich dir ein Szenario: Angenommen, die Anna benützt ihr Handy immer nur zu Hause
156 und alleine, ohne, dass sich jemand anderer sich im gleichen Raum aufhält oder neben ihr ist.
157 Meinst du, dass es dann trotzdem möglich ist, dass andere ihre Fotos sehen können, obwohl
158 sie es ihnen weder zeigt noch schickt?
159 I: Ja.
160 A: Wie?
161 I: Keine Ahnung.
162 A: Aber du hältst es für möglich.
163 I: Ich denke schon.
164 A: Gibt es einen Grund, wieso du denkst, dass das schon möglich sein kann.
165 I: Ich glaube auch, wenn wir heute so ein Smartphone haben, wenn jemand will, dann könnten
166 sie uns auch orten, oder alle unsere Kontakte runterladen.
167 A: Kannst du dir vorstellen, dass die Anna ihnen das sogar erlaubt, zuzugreifen, aber ihr das
168 nicht wirklich bewusst ist, dass sie die Erlaubnis erteilt hat.
169 I: Ja, wenn man dieses blöde Ding nicht durchgelesen hat. Die Nutzungsbedingungen.

170 A: Wie gut sind deine Fotos auf deinem Smartphone vor der Einsichtnahme anderer Leute
171 geschützt?

172 I: Dass andere auf meine Fotos Zugriff haben?

173 A: Ja.

174 I: Also, wenn du so fragst, dann denke ich nicht gut.

175 A: Und wieso nicht?

176 I: Du darfst mir diese Frage nicht stellen. (lacht)

177 A: Ja, das kann ja sein, dass du sagst, ich glaube eigentlich schon gut, weil...

178 I: Also ich mach mich da ganz locker, weil ich sowieso denke bei meinem Smartphone ist
179 nichts sicher, weil wenn sich jemand da ein bisschen auskennt, wie was zu tun ist, dann kann
180 er alles von meinem Handy haben. Also ich habe keine Zweifel, dass wenn jemand möchte,
181 dass er dann Fotos, Daten, was weiß ich was alles, runterladen könnte von meinem Handy.

182 A: Hast aber irgendwie keine Fotos zum Beispiel, bei denen du sagst, da möchte ich nicht,
183 dass diese irgendjemand anderer sieht?

184 I: Nein.

185 A: Was müsste passieren, dass du sagst ich lösche diese App, weil...

186 I: Was da passieren müsste? Ja, wenn ich wirklich Fotos auf meinem Smartphone hätte, bei
187 denen ich nicht möchte, dass sie andere sehen, dann müsste das passieren. Aber jetzt im
188 Moment denke ich mir, wäre mir das egal.

189 A: Was heißt, passieren?

190 I: Dass die öffentlich werden.

191 A: Dass du sie in der Zeitung siehst?

192 I: Ja, wie das. Da hab ich mir gedacht, jaja, das war mein Profelfoto, aber wenn ich da
193 halbnackt oben wäre, oder ganz, dann hätte ich ein Problem damit.

194 A: Mhm, außer Fotos, sonst noch was?

195 I: Ja oder wenn jemand von meinem, ich weiß nicht, ob das jetzt mit dem Handy zu tun hat
196 oder mit Google. Ich meine, wenn jemand meine A-Mailadresse hackt und von meinen E-
197 Mailaccount so E-Mails rausschickt, wo man Geld oder irgendwas fordert, wo ich auch schon
198 mal so eine E-Mail gekriegt habe, dann ist das für mich etwas, wo ich die E-Mails wieder
199 löschen muss, weil sowas geht logisch nicht, wenn jemand in meinem Namen Sachen
200 verschickt.

201 A: Dein Ruf praktisch geschädigt wird.

202 I: Ja.

203 A: Wer bestimmt jetzt deine Sicherheit von deinen Fotos und Daten auf deinem Handy?

204 I: Wer?

205 A: Ja.

206 I: Wahrscheinlich ich.

207 A: Und wie? Oder wieso du und nicht jemand anderer?

208 I: Also mein Handy, also meine Daten, deswegen.

209 A: Ok. Kannst du das auch irgendwie kontrollieren wer oder welche App worauf Zugriff hat?

210 I: Ob ich das kontrollieren kann? Ich denk, wenn man möchte schon. Oder? Das muss ja auch

211 Richtlinien haben, nach denen sie arbeiten dürfen. Und wenn du diese Infos haben möchtest,

212 kannst du das sicher ausfindig machen.

213 A: Könntest du dir auch vorstellen, dass du unter den Einstellungen von deinem Handy schon

214 siehst, wer auf was Zugriff hat und wer wie viel von was nimmt?

215 I: Ma, das weiß ich jetzt nicht.

216 A: Wie erhalten die Apps den Zugriff, dass sie deine Fotos hernehmen dürfen?

217 I: Weil ich ihnen die Erlaubnis gib, wenn ich die Apps herunterlade.

218 A: Wieso meinst du, brauchen diese Zugriff auf verschiedene Bereiche?

219 I: Hm. Ich denk jetzt immer an eine App, damit ich ein Beispiel habe, sonst kann ich dir diese

220 Frage nicht beantworten.

221 A: Ok.

222 I: Jetzt wenn ich denke an WhatsApp, dann brauchen die Zugriff auf meine Kontaktliste,

223 sonst hätte ich die Nummern nicht drinnen in WhatsApp, oder? Schon vom logischen, das

224 vielleicht. Oft dafür, dass ich sie überhaupt benutzen kann, das was ich benutzen möchte und

225 der Rest ist damit, ich glaube sie könnten auch mit einem bestimmten Foto, das sie von mir

226 nehmen, werben. Da hätten sie das Recht dazu. Und auch wenn sie 1.500€ verdienen würden,

227 dann hätten sie das Recht dazu.

228 Du hast mich gefragt warum, oder?

229 A: Ja, wieso die auf verschiedene Bereiche Zugriff brauchen. Wenn wir uns jetzt vorstellen,

230 du hast eine Taschenlampen-App drauf, hast du gesagt. Kannst du dir vorstellen, dass die

231 Taschenlampen-App sagt, sie braucht Zugriff auf die Fotokamera, um zu funktionieren?

232 I: Nein.

233 A: Wieso nicht?

234 I: Auf die Fotokamera? Ah, das schon. Sonst könnte die Taschenlampe ja gar nicht leuchten.

235 Ja, sie braucht das Licht, oder da, wo das Licht rauskommt.

236 A: Den Blitz oder so meinst du?

237 I: Ja.

238 A: Kannst du dir vorstellen, sie sagt, sie braucht Zugriff auf das Tonband, damit sie
239 funktionieren kann?

240 I: Auf das Tonband? Nein, macht die Lampe Geräusche?

241 A: Sagen wir mal nein, sie macht keine Geräusche.

242 I: Dann nicht.

243 A: Wieso nicht?

244 I: Weil sie dann keinen Ton braucht.

245 A: Wieso meinst du, könnte sie sonst noch den Zugriff verlangen auf das Tonband, dass sie es
246 ein und ausschalten kann?

247 I: Die Lampe?

248 A: Wenn du die Taschenlampen-App runterladest und es steht in den Bedingungen, sie
249 braucht Zugriff auf das Tonband und kann es automatisch ein und ausschalten. Wenn es jetzt
250 zum Beispiel heißt, sie braucht das nicht, um eine Funktion ausführen zu können, wieso
251 könntest du dir vorstellen, braucht sie sonst Zugriff auf das Tonband?

252 I: Weil sie wollen selbst eine App mit Taschenlampen machen.

253 A: Wer?

254 I: Keine Ahnung, die von der Taschenlampen-App.

255 A: Eine App mit Tonband dann machen?

256 I: Ja.

257 A: Und wenn die Taschenlampen-App sagt, sie braucht Zugriff auf das Internet, dass sie das
258 braucht, um funktionieren zu können?

259 I: Ich wüsste das gar nicht, ob die App funktionieren würde ohne Internet, wenn sie keine
260 Verbindung zum Internet hätte. Ich glaube sie geht doch.

261 A: Und wieso geht die App dennoch, ohne Internet?

262 I: Keine Ahnung. Braucht die Internet? Weißt du, ich benütz die Taschenlampe nicht so oft.

263 A: Ok. Gut, dann: Was können Apps machen, wenn sie zum Beispiel den Zugriff auf deine
264 Fotos, auf dein Adressbuch, auf deine Foto- und Videokamera? Was können sie machen,
265 wenn sie da überall Zugriff haben?

266 I: Was können die machen? Ich weiß es nicht.

267 A: Ok. Nehmen wir, an die Anna ladet sich eine App runter und akzeptiert bei der
268 Installation, dass die App zugreifen kann auf ihre Fotos, ihr Adressbuch, die Foto- und
269 Videokamera ein und ausschalten kann, Internet auch. Die App speichert sich dann alle
270 Informationen, welche die Anna drauf hat, worauf die App Zugriff hat, herunter. Welche
271 Folgen könnte das für die Anna haben, dass die App einfach alles über die Anna weiß?

272 I: Welche Folgen? Hm. Die haben praktisch Daten, Foto, alles?
273 A: Ja.
274 I: Ja, dass die Daten, Fotos ausgenutzt werden können. Wenn. Keine Ahnung. Für etwas zu
275 werben, für Geld zu verdienen, Kontakte zu nutzen.
276 A: Was bringt ihnen das?
277 I: Meistens Geld. Also ich denk mir, wenn, dann ist das das Ziel.
278 A: Was können Unternehmen machen, wenn sie unzählig viele Daten von unzählig vielen
279 Leuten besitzen? Was ist da der Gedanke dahinter?
280 I: Werbezwecke? Würde ich jetzt so spontan sagen. Nein ich weiß es nicht.
281 A: Sonst noch irgendwas? Was sie mit den Daten alles machen können? Oder wie benützen
282 sie diese Daten für die Werbung?
283 I: Ja keine Ahnung, entweder da sind E-Mails drauf, dann kannst du E-Mail-Werbung
284 machen, oder sonst Telefonnummern, das weiß ich jetzt nicht. Oder sie verkaufen die
285 Kontakte, das könnte auch sein.
286 A: Wer oder wieso könnte da überhaupt jemand interessiert sein, die Kontakte zu kaufen?
287 I: Ja zum Werben. Immer!
288 A: Hast du dir schon überlegt, einen Dienst aufzugeben, weil er zu viele Daten von dir
289 gespeichert hat?
290 I: Ja, überlegt schon.
291 A: Was muss zum Beispiel für dich passieren, dass du sagst, Facebook, das lösche ich jetzt, das
292 reicht jetzt.
293 I: Was muss passieren? Ja ich glaub, das ist die gleiche Antwort wie vorhin. Wenn Facebook
294 hergeht und irgendein Foto verwenden würde und, keine Ahnung, was damit anstellt.
295 A: Wie möchtest du dich in Zukunft vor der Datenspeicherung schützen?
296 I: Ich lese mir jetzt das was ich akzeptiere durch.
297 A: Ja, super, das ist schon mal ein guter Weg.
298 A: Wie denkst du wird unser Leben mit dem Smartphone in 30, 50 Jahren aussehen?
299 I: Hm. Ja, ich denk mir einmal, es wird halt noch mehr, alles mit dem Handy oder mit einer
300 neuen Sache, einer neuen Technologie gemacht.
301 A: Jetzt sag ich dir ein paar Szenarien und du musst sagen, ob diese für dich realistisch sind
302 und warum. Wenn jemand täglich das Smartphone mit Apps und Internet nutzt, und da zum
303 Beispiel Twitter und/oder Facebook, aber er jedoch nie seinen Standort angibt. Ist es für dich
304 dann realistisch, dass man doch mit großer Wahrscheinlichkeit vorhersagen kann, wo sich
305 derjenige in Zukunft aufhalten wird?

306 I: Ja.
307 A: Wieso?
308 I: Weil ich eben glaube, dass man orten kann, das Handy orten kann, also die Person.
309 A: Und kannst du dir auch vorstellen, dass wenn der- oder diejenige das Handy verliert, sagen
310 wir mal, dass man nur durch die Freunde auf Facebook sich schon irgendwie ausrechnen
311 kann, mit einer Wahrscheinlichkeit, wo sich diese Person in Zukunft aufhalten wird?
312 I: Ja.
313 A: Wieso das?
314 I: Ja weil die Freunde könnten ja irgendwie wohl auch mich selbst mit posten, wenn sie ein
315 Foto machen und ich drauf bin und sie das dann mit Standort posten, dann wissen sie ja wo
316 ich bin.
317 A: Und wenn das auch nicht der Fall ist. Wenn nur die Freunde praktisch ihren Standort
318 angeben, aber nie in Verbindung jetzt zum Beispiel mit dir auf Facebook aufscheinen.
319 I: Das könnten sie rein theoretisch, wenn sie gut sind. Ja, glaub ich schon, dass sie das im
320 Stande sind.
321 A: Wie würde das funktionieren?
322 I: Du, ich glaub das ist nicht schwer. Logisch hast du hunderte Freunde auf Facebook, aber
323 wenn man dann wirklich alle Daten hat und mitkommt, und alles ein bisschen verfolgt, was
324 da abgeht, dann kann man glaub ich schon daraus schließen, wo diese Person ist. Weil wenn
325 ich bei Firma1 arbeite, das bekommt der ja mit auf Facebook. Und wenn ich zig Freunde von
326 Firma1 auf Facebook habe und jemand postet, das ist das Wochenende, dann könnte er davon
327 ausgehen, dass ich dieses Wochenende auch dort bin. Könnte sein.
328 A: Hast du schon einmal davon gehört, dass das möglich sein sollte?
329 I: Nicht jetzt in Form von Zukunft, sondern nur, wenn jemand das Handy mit sich hat.
330 A: Wie realistisch ist es für dich, dass die Polizei schon heute wissen kann, wo morgen ein
331 Verbrechen stattfindet? Nehmen wir mal eine größere Stadt her, nicht unbedingt Ort4 oder
332 Ort1, ist das für dich realistisch, dass sich das die Polizei schon ausrechnen kann?
333 I: Hm. Das weiß ich jetzt nicht, könnte sein, wenn sie sagt, da und da ist ein Verbrechen. Ok.
334 In welcher Art?
335 A: Egal.
336 I: Ok, weil ich habe jetzt an eine Party gedacht, dann artet diese aus, könnte theoretisch sein.
337 A: Ja.
338 I: Jetzt. Ob Mord oder so, das weiß ich nicht, das denke ich nicht.
339 A: Wieso nicht?

340 I: Ja, weil das doch nicht immer berechenbar ist, sonst denke ich mir, würden sie sicher viel
341 verhindern.

342 A: Wieso hältst du das nicht für berechenbar?

343 I: Ich denke es kommt jetzt auf das Beispiel des Verbrechens drauf an. Denke ich da zu
344 kompliziert?

345 A: Sag einfach mal.

346 I: Nehmen wir mal an ein Verbrechen: Überfall. Dass sie das vorhersagen können, glaube ich
347 jetzt nicht. Wenn sie sagen, ich halte morgen ein Verbrechen auf, glaube ich nicht, dass sie
348 das rausfinden können, außer sie ermitteln schon an einem Fall.

349 A: Könntest du dir vorstellen, dass sie jetzt nicht mal genau wissen, welches Verbrechen das
350 sein wird, sondern mehr dass sie wissen, ok, in dieser Gegend wird morgen mit dieser
351 Wahrscheinlichkeit ein Verbrechen stattfinden, in der anderen Gegend ist es schon etwas
352 unwahrscheinlicher, und dort ist sie ganz hoch.

353 I: Ja, ok, das denke ich schon. Weil ich meine in einer Stadt gibt es ja auch Orte, wo viele
354 Sachen passieren. Wo Armut herrscht und Kriminalität usw.. Das kannst du dir schon
355 ausrechnen, hingegen in anderen Bereichen weniger.

356 A: Wie kann man sich das ausrechnen?

357 I: Ja, ich weiß nicht, aber in einer großen Stadt weiß man ja wo die Armutsviertel sind, die
358 Ghettos und so. Wo schon manchmal was war. Du meinst nur mit dem Smartphone, oder?

359 A: Nein, generell mit den Daten.

360 I: Mit den Daten?

361 A: Das heißt, wenn du dir ansiehst, wo früher überall Verbrechen stattfanden, dann kannst du
362 dir das ausrechnen wo sie wieder stattfinden werden?

363 I: Ja, das hätte ich mir jetzt gedacht.

364 A: Gut, dann das dritte Beispiel: Nehmen wir an eine Frau kauft im Supermarkt verschiedene
365 Sachen ein, darunter jedoch keinerlei Babysachen. Kannst du dir vorstellen, dass man nur von
366 den gekauften Artikeln mit hoher Wahrscheinlichkeit sagen kann, ob diese Frau schwanger ist
367 oder nicht und ungefähr auch den Geburtstermin feststellen kann?

368 I: Echt jetzt? Du hast ja Szenarien. Ob man das kann?

369 A: Ja.

370 I: Hm. Den Geburtstermin, nein das glaube ich jetzt nicht, bitte nicht.

371 A: Aber rein, ob die Frau schwanger ist oder nicht schon?

372 I: Ja, sie darf nichts Rohes essen, aber das... ja man weiß ja nicht, ob sie nur für sich einkauft,
373 oder für zwei. Also ich glaube nicht.

374 A: Wieso nicht?
375 I: Ja, weil sie für sich und mehrere einkaufen kann.
376 A: Und wenn sie das vorher auch schon immer getan hat?
377 I: Für mehrere eingekauft?
378 A: Ja. Also kannst du dir nicht vorstellen, dass wenn man im Supermarkt einkauft, dass es
379 dann möglich ist, dass man herausfinden kann, ok, diese Frau könnte schwanger sein. Oder im
380 Grunde auch der Mann, wenn er für die Frau einkauft. Ist im Prinzip das gleiche.
381 I: Glaub ich nicht.
382 A: Ok.
383 A: Nehmen wir an, ein Mann ist homosexuell, er nützt das Internet, darunter auch Social
384 Media, Facebook usw., gibt jedoch nirgends an, dass er Männer liebt. Er hält sein Sexualleben
385 auch geheim, gibt also weder im Internet, noch sonst irgendwo an, dass er homosexuell ist.
386 Für wie realistisch ist es für dich, dass wildfremde Personen dennoch mit hoher
387 Wahrscheinlichkeit sagen können, dieser Mann ist schwul?
388 I: Ja, manchmal sieht man es jemandem ja an, oder? Und dann braucht er nur Fotos posten
389 und dann kann sich der andere denken, ok, der wird schwul sein. Oder in Locations, wo er
390 sich aufhält, vielleicht gibt er diese an und man weiß vielleicht welche Szene sich da
391 rumtreibt und man vermutet dann, dass dieser Mann schwul sein könnte.
392 A: Das heißt, es werden Daten kombiniert? Oder wie funktioniert das dann? Könntest du dir
393 das vorstellen?
394 I: Ja.
395 A: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft deine Freundesliste auf Facebook
396 kontrollieren und auch die Bewegungsdaten von deinem Smartphone prüfen, wenn sie
397 schauen wollen, ob du kreditwürdig bist oder nicht und welchen Kredit du überhaupt
398 bekommst?
399 I: Echt wahr, über Facebook? Wie soll denn das gehen? Dann brauchen sie ja meine Bank, ich
400 mach über Facebook doch nicht meine Geldgeschäfte.
401 A: Könntest du dir vorstellen, dass das Kreditinstitut hergeht und schaut, mit wem bist du
402 befreundet?
403 I: Ok. Könnte sein, ja.
404 A: Wieso?
405 I: Ja, mit wem du dich umgibst, das sagt ja auch etwas über dich aus. Vielleicht sieht man, der
406 hält sich in besseren Kreisen auf, der in weniger guten.
407 A: Macht das schon Aussagen?

408 I: Ja.

409 A: Du hast gesagt, du hast auch so Gesundheits- und Fitness-, Sport-Apps. Kannst du dir
410 vorstellen, dass in Zukunft Gesundheitsversicherungen sich mit solchen Apps
411 zusammenschließen, wenn sie schauen, ob du regelmäßig Sport machst und ob du dich
412 gesund ernährst, wenn du eine Versicherung bekommst oder welche Versicherung sie dir
413 anbieten?

414 I: Ob sie das können?

415 A: Genau, ob du dir das vorstellen kannst, dass sie das machen.

416 I: Ja.

417 A: Wieso sollten sie das machen?

418 I: Ja, weil dann können sie genau schauen, welche Versicherung sie anbieten können. Und je
419 gezielter sie schießen, umso eher wird der dann Kunde. Je mehr Informationen sie über mich
420 haben, desto gezielter können sie mir ein Produkt verkaufen und desto eher ist die
421 Wahrscheinlichkeit, dass ich Kundin werde.

422 A: Kannst dir auch vorstellen, dass das mit ihrer Sicherheit irgendwie zu tun hat? Dass sie
423 sagen, ich muss mich auch irgendwie absichern, weil, wenn ich ihr eine sehr günstige
424 Versicherung gebe und sie ist dann in den nächsten fünf Jahren krebskrank oder so etwas,
425 dass sie das dann damit überprüfen?

426 I: Ja.

427 A: Wenn du, sagen wir mal in die USA, oder ein Land, einreisen möchtest, könntest du dir
428 vorstellen, dass nur durch ein Wort das du im Internet eingibst oder in einer SMS schreibst,
429 dass du dadurch nicht mehr in ein Land einreisen darfst?

430 I: SMS oder in einem Wort? Ja! Glaube ich.

431 A: Wieso?

432 I: Weil das als Schutz vor Terroranschlägen dient.

433 A: Hast du schon einmal davon gehört?

434 I: Wo?

435 A: Keine Ahnung. In den Nachrichten?

436 I: Ja, das kann sein.

437 A: Kannst du dir vorstellen, dass man aus dem Verhalten der Vergangenheit, das Verhalten in
438 der Zukunft schon vorhersagen kann?

439 I: Vorhersagen ist schwierig, aber man kann mit hoher Wahrscheinlichkeit sagen, dass ...

440 A: Wieso?

441 I: Ich kann mich grundlegend ändern, aber das passiert meistens nicht auf eins, zwei.

- 442 A: Aber eine Wahrscheinlichkeit besteht, dass man gleich bleibt oder in diese Richtung
443 tendiert.
- 444 I: Ja, und sonst verändert es sich langsam.
- 445 A: Gut, Danke, das war's. Danke für das Interview.

1 **Interview 8, 28.10.2014. Dauer 32:03 Minuten**

2

3 A: Wie alt bist du, und was machst du beruflich?

4 I: Ich bin 21 und bin zur Zeit Beruf 6.

5 A: Mit welchen Medien informierst du dich vorwiegend?

6 I: Internet oder Zeitschriften kann man auch sagen.

7 A: Was verwendest du da vor allem?

8 I: Bei den Zeitschriften vor allem die Zeitung oder die Tageszeitung. Und beim Internet, da
9 bin ich eigentlich, Google-Suchmaschine.

10 A: Hast du zum Beispiel beim Internet auch Online Ausgaben von Zeitungen oder so, dass du,
11 Spiegel Online oder Onlineausgaben?

12 I: Nein.

13 A: Bei Facebook hast du dort zum Beispiel immer wieder Aktualisierungen von Stol zum
14 Beispiel?

15 I: Ja, Stol.

16 A: Dann Radio?

17 I: Ja, Radio höre ich auch sehr viel, überhaupt beim Autofahren, da hör ich immer Radio.

18 A: Auch die Nachrichten dort?

19 I: Ja, auch die Nachrichten.

20 A: Wie sieht es mit Fernsehen aus?

21 I: Fernsehen schau ich auch, aber da nicht unbedingt die Nachrichten, vielleicht mal Sendung
22 1oder so, aber das sind ja nicht richtige.

23 A: Ja, mehr so Klatsch und Tratsch.

24 I: Klatsch und Tratsch, ja.

25 A: Nutzt du diese Medien täglich?

26 I: Ja, eigentlich schon.

27 A: Welches Smartphone besitzt du?

28 I: Marke 2.

29 A: Für was gebrauchst du dein Smartphone?

30 I: Vor allem zum Kommunizieren, mich mit anderen Leuten in Kontakt zu setzen, zu telefonieren,
31 SMS schreiben, oder auch schnell auf dem Weg mal was zu recherchieren, wenn ich was brauche.
32 Über den Weg, oder wenn ich etwas sehe, und ich möchte wissen, was das ist, dann halt da
33 nachzuschauen.

34 A: Also Internet?

35 I: Ja, Internet, kann man schon sagen.
36 A: Hast du auch so Geburtstagskalender zum Beispiel?
37 I: Nein, eigentlich nicht.
38 A: Hast du auch Apps heruntergeladen?
39 I: Ja, Apps habe ich heruntergeladen.
40 A: Und was hast du da welche?
41 I: Zum Beispiel, jetzt, TV-Magazin, Stol habe ich, Facebook, Facebook-Messenger,
42 WhatsApp. Die Sachen, die man halt so hat.
43 A: Hast du auch Spiele zum Beispiel?
44 I: Nein, Spiele habe ich keine.
45 A: Taschenlampe?
46 I: Taschenlampe ist schon drauf.
47 A: Wetter-App?
48 I: Wetter-App, nein, aber die Südtirol-App habe ich oben, über Wanderwege und wo man halt
49 alles rausfinden kann.
50 A: Sonst so Shopping-Apps oder Kalender?
51 I: Kalender ist auch schon oben und Shopping-App verwende ich keine.
52 A: Gut, wie oft verwendest du diese Apps? Oder welche verwendest du besonders und wie oft?
53 I: Ja, Facebook und WhatsApp benutze ich täglich und Stol, das benutze ich täglich
54 eigentlich, und die anderen benutze ich einmal die Woche, zweimal die Woche, ist sicher
55 unterschiedlich, gerade welche man braucht.
56 A: Hast du auch so Fotokamera, wo du Fotos bearbeiten kannst, heruntergeladen?
57 I: Nein, habe ich nicht heruntergeladen.
58 A: Hast du den Begriff Big Data schon einmal gehört?
59 I: Nein.
60 A: Kannst du dir ungefähr vorstellen, was man darunter versteht?
61 I: Irgendein Datennetzwerk, keine Ahnung.
62 A: Ok. Datenschutz ist dir das ein Begriff?
63 I: Ja, das schon.
64 A: Wie gut kennst du dich mit Datenschutz aus?
65 I: Sagen wir recht, ja ein bisschen.
66 A: Erzähl mal: Wenn du jemanden erklären müsstest, was Datenschutz ist, was würdest du
67 dann sagen?

68 I: Ja das ist halt, zum Beispiel wenn ich irgendwo meine Daten eingeben muss, ist immer ein
69 Datenschutz dabei, den ich dann bestätigen muss oder unterschreiben muss, dass meine Daten
70 nicht weitergegeben werden. Also sie bestätigen mir gegebenenfalls in diesem Fall, dass diese
71 Daten nur für bestimmte Zwecke benutzt werden und nicht veröffentlicht werden oder
72 missbraucht werden.

73 A: Was wären solche Fälle, für welche sie sie benutzen könnten?

74 I: Studien zum Beispiel, oder ja.

75 A: Was untersuchen sie da, weißt du das ungefähr?

76 I: Wahrscheinlich Nachfragen, oder wie sich der Markt entwickelt, oder, keine Ahnung. Denk
77 ich mir halt, weiß nicht.

78 A: Also Datenschutzrichtlinie ist dir ein Begriff, richtig?

79 I: Ja.

80 A: Und was in einer solchen Datenschutzrichtlinie drinnen steht, weißt du auch?

81 I: Ja, für was meine Daten verwendet werden.

82 A: Wo hast du denn schon mal eine unterzeichnet?

83 I: Ma, das macht man eigentlich oft, oder? Wo es einem oft auch nicht bewusst ist.

84 A: Wo zum Beispiel? Was fällt dir jetzt so ein?

85 I: Was fällt mir jetzt so ein? Zum Beispiel, wenn ich bei einem Gewinnspiel teilnehme, da
86 muss man ja auch immer unterschreiben, da ist ja auch Datenschutz dabei. Oder wenn man
87 sich bei einem Verein, zum Beispiel Mitglied wird, dann ist ja auch meistens ein Datenschutz-
88 Dings dabei. Auch wegen Fotos, ob sie Fotos veröffentlichen dürfen oder nicht.

89 A: Wenn wir nun an deine Apps denken, meinst du, haben diese eigene
90 Datenschutzrichtlinien?

91 I: Ja, haben tun sie sie schon, aber man liest sie sich nie durch, oder?

92 A: Hast du dir mal eine halbwegs durchgelesen, oder vollständig?

93 I: Eine hab ich mal angefangen durchzulesen, aber ich habe gleich mal aufgegeben.

94 A: Ok. Weil?

95 I: Weil ich mir gedacht habe, ja ist gleich. Man ist ein bisschen nachlässig, ich weiß.

96 A: War es zu anstrengend es durchzulesen, oder zu kompliziert?

97 I: Zu kompliziert und zu lang.

98 A: Welche Datenschutzrichtlinien, meinst du, haben deine Apps?

99 I: Dass die Daten nur für sie verwendet werden. Also für das Unternehmen, das die App hat,
100 dass die Daten, dass da halt bestätigt wird, dass die Daten nur bei ihnen bleiben, so zu sagen.

101 A: Wo kannst du dich über diese Datenschutzrichtlinie z.B. informieren von Apps?

102 I: Die müssten. Die müssten wohl immer irgendwo drinnen sein, oder? Wenn du bei den
103 Einstellungen schaust, müsste immer irgendwo auch Datenschutz stehen. Oder?
104 A: Das klären wir eventuell nachher.
105 Auf welche Daten können Apps zugreifen?
106 I: Das ist glaube ich immer unterschiedlich. Glaube ich halt. Also halt auf jeden Fall, das was
107 du eingibst, das haben sie wohl immer schon und manche Daten von manchen Apps musst du
108 auch einstellen, ob sie auf deine Fotos zugreifen dürfen oder nicht. Aber das kannst du auch
109 oft freiwillig einstellen.
110 A: Aber was sind dann so bestimmte Bereiche, auf die sie zugreifen können? Foto hast du
111 gesagt.
112 I: Foto, ja meine ganzen Daten, meine ganzen Nachrichten wahrscheinlich auch. Wenn ich
113 zum Beispiel an die Nachrichtenportale denk, weißt du wie so Chats oder so, können sie
114 sicher auch darauf zugreifen.
115 A: Ok. Sonst auch irgendwas, Adressbuch?
116 I: Sicher auch.
117 A: Du hast gesagt, du nutzt dein Smartphone auch um Fotos zu machen, richtig?
118 Nehmen wir mal an, die Anna nutzt ihr Handy immer nur zu Hause und alleine, ohne, dass
119 sich jemand anderer neben ihr oder im gleichen Raum aufhält. Denkst du, ist es dann dennoch
120 möglich, dass wildfremde Personen dennoch Zugriff auf ihre Fotos und Daten haben, ohne
121 dass sie es ihnen zeigt oder schickt?
122 I: Eine Möglichkeit gibt es sicher immer. Also wenn jemand unbedingt will die Foto von ihr
123 haben, dann sage ich, und er ist ein bisschen intelligent, der das auch kann, dann sage ich gibt
124 es sicher immer eine Möglichkeit. Weil irgendwie mit dem Handy ist man immer irgendwie
125 verletzbar, auch wenn man es nicht will. Denk ich mir.
126 A: Mhm, kannst du dir auch vorstellen, dass sie das zum Beispiel denjenigen sogar erlaubt,
127 ihr das aber eigentlich nicht bewusst ist, dass sie es erlaubt, dass derjenige Zugriff auf ihre
128 Daten hat?
129 I: Ja.
130 A: Wie könntest du dir das vorstellen?
131 I: Ja, durch das, dass man die Datenschutzrichtlinien nie durchliest, eigentlich, glaube ist da
132 immer eine Hintertür, wo sie sich das beschaffen können auch ohne, dass man sich das
133 überhaupt bewusst ist.
134 A: Aber ganz legal dann?
135 I: Ja, ganz legal.

136 A: Wie gut sind deine Fotos auf deinem Smartphone vor der Einsichtnahme anderer Leute
137 geschützt?

138 I: Also dort wo ich es schützen kann, sagen wir mal zum Beispiel, du kannst dich ja schützen,
139 indem du auf Facebook oder WhatsApp sperrst, dass sie nicht auf deine Fotos zugreifen.
140 Wenn du es nicht sperrst, dann können sie ja eigentlich, rein theoretisch, immer alle sehen.
141 Das ist mal eine Möglichkeit mit der man sich schützen kann.

142 A: Ok, es gibt sicher noch mehr Möglichkeiten, sich noch mehr zu schützen. Das heißt: Hast
143 du jetzt wirklich die Apps kontrolliert, dass du wirklich weißt, ok diese Apps können
144 zugreifen oder nur diese eine kann zugreifen? Weißt du das?

145 I: Also bei ein paar weiß ich das schon, also, dass sie, ich bin im Glauben, dass sie nicht
146 zugreifen können. Ob das dann stimmt oder nicht, das ist ...

147 A: Ok, kannst du das auch kontrollieren wer jetzt Zugriff hat und wer nicht?

148 I: Nein, also...

149 A: Siehst du das nirgends auf deinem Smartphone?

150 I: Nein, mitbekommen tust du das nicht, ob jetzt jemand zugreift oder nicht.

151 A: Wer bestimmt die Sicherheit von deinen Daten, deiner Fotos auf deinem Handy?

152 I: Bestimm, das tust du wohl eigentlich selber, denke ich mir. Oder ich versuche es selber zu
153 bestimmen, sagen wir so.

154 A: Ja, im Grunde, wer hat – außer dir – noch alles Zugriff auf deine Fotos, deine
155 Kalendernotizen, dein Adressbuch, deine Daten?

156 I: Meinst du jetzt von den Apps aus gesehen?

157 A: Zum Beispiel.

158 I: Ja Zugriff hat sicher fast jeder App-Anbieter.

159 A: Und wie genau erhalten sie diesen Zugriff?

160 I: Durch den, dass ich mich bei Ihnen registriere und anmelde und sagen wir so, wenn
161 irgendwo eine Sicherheitslücke drinnen ist im Datenschutz, dann auf jeden Fall schon. Aber
162 es ist ja so, bevor man das nicht unterschreibt, kommt man ja eh nirgends mehr weiter. Also
163 man kriegt ja Apps nicht, ohne das zu unterschreiben.

164 A: Das heißt aber eigentlich erlaubt man ihnen das mit den Datenschutzrichtlinien selbst?

165 I: Manchmal schon, ja.

166 A: Wieso meinst du brauchen Apps Zugriff auf verschiedene Bereiche? Fotos, Adressbuch,
167 Kalender, was auch immer?

168 I: Damit sie besser funktionieren können. Man will ja dass alles, dass man nirgendwo mehr
169 muss alles eintippen, dass sich das schon alles selbst aktualisiert, deswegen ist man ja selbst

170 schuld, von mir aus gesehen. Man will es ja immer gemütlich haben, dass wenn ich da
171 reingehe, möchte ich, dass es automatisch das Adressbuch rauflädt, und deswegen sagt man ja
172 selbst eigentlich, dass sie das dürfen.

173 A: Kannst du dir noch irgendwie einen Nutzen für die App vorstellen, wenn sie auf deine
174 Daten Zugriff haben?

175 I: Irgendeinen Nutzen muss es für sie schon haben, ja. Ich weiß es aber nicht was.

176 A: Nehmen wir mal an die Wetter-App.: Wieso, meinst du, braucht die Wetter-App Zugriff
177 auf das Internet, damit sie funktionieren kann?

178 I: Wie meinst du das jetzt?

179 A: Wieso meinst , steht bei der Wetter-App in den Datenschutzrichtlinien sie braucht Zugriff
180 auf das Internet?

181 I: Ah, ja weil sie das aktualisieren müssen, sonst ginge das ja nicht. Ich muss ja jeden Tag
182 wissen, wie das Wetter wird und wenn sie nicht mit dem Internet verbunden wäre, dann kann
183 mein App das ja nicht aktualisieren. Dann wäre rein theoretisch jeden Tag das gleiche Wetter
184 bei mir.

185 A: Und wieso meinst du, schreibt die Wetter-App in der Datenschutzrichtlinie, sie braucht
186 Zugriff auf das Adressbuch?

187 I: Irgendeinen Nutzen müssen sie haben. Vielleicht wollen sie, keine Ahnung. Verstehe ich
188 auch nicht, wieso eine Wetter-App Zugriff auf die Adressen braucht. Weil das...

189 A: Auf die Fotos zum Beispiel.

190 I: Für Werbung vielleicht. Keine Ahnung.

191 A: Wie würde das mit der Werbung funktionieren?

192 I: Ja es gibt ja auch Fälle, wo sie einfach Fotos benützen von einem und dann für eine
193 Werbung einsetzen, ohne dass du eigentlich... Du hast ja eigentlich deine Zustimmung
194 gegeben, aber du weißt es eigentlich nicht mal.

195 A: Das heißt, welche Gründe gibt es für die Unternehmen von den Apps, dass sie den Zugriff
196 auf diese verschiedenen Daten brauchen, obwohl sie jetzt für die Funktion von der App nicht
197 ausschlaggebend sind?

198 I: Wenn ich das wüsste, dann würde ich es dir gerne sagen.

199 A: Wenn du dir jetzt vorstellst, eine App hat unzählig viele Daten, nicht nur von dir, sondern
200 von ganz, ganz vielen Leuten. Was könnten dann die Folgen für uns sein, wenn diese alles
201 über uns wissen, also nicht nur über uns zwei, sondern über uns alle.

202 I: Erpressung, Ausnutzung. So irgendwas.

203 A: Mhm. Und wie könnten sie das machen? Wie machen sie diese Erpressung oder
204 Ausnutzung? Wie würde das funktionieren?

205 I: Mit, keine Ahnung, Verträge oder irgendwas, dass sie sagen, schau ich habe das und das
206 von dir. Du musst das und das. Vor allem bei den Bankdaten muss man sich sehr aufpassen
207 meiner Meinung nach. Da können sie ja auch das ausnutzen und dir irgendeine Klausel
208 dreingeben, wo du sagst, da habe ich gar nie zugestimmt, aber im Grunde hast du es nie
209 durchgelesen.

210 A: Meinst du jetzt auch Kreditkarten, wenn du diese angibst, dass sie dir dann immer was
211 abbuchen, was du aber eigentlich gar nicht möchtest.

212 I: Genau. Es heißt zwar immer, es sei gratis, die Nutzung zum Beispiel, aber dann musst du
213 alles angeben. Und es heißt zwar, es werde nicht belasten, aber dann im Kleingedruckten steht
214 wieder was anderes und solche Sachen. Ja.

215 A: Das heißt, wie werden die Daten von der App dann weiterverarbeitet, wenn sie Zugriff
216 haben auf dein Handy?

217 I: Da bin ich jetzt überfragt.

218 A: Ok, hast du dir auch schon mal überlegt einen Dienst oder eine App zu kündigen, weil du
219 gesagt hast, die greifen auf zu viele Daten von mir zu und ich kann das nicht kontrollieren?

220 I: Ja, eine habe ich gekündigt. Das war auch so eine Nachrichten, so ein Messenger so zu
221 sagen, aber die war mir zu, da waren, ich weiß nicht mehr, so komische Hinweise oder so was
222 und das ist mir komisch vorgekommen. Wo man alle möglichen Daten eingeben hätte sollen.
223 Die habe ich dann gelöscht.

224 A: Auf was hätte diese dann Zugriff gehabt, du hättest dich mit allen möglichen anmelden
225 müssen. Auch zum Beispiel, dass die das Tonband automatisch ein und ausschalten kann und
226 so was?

227 I: Solche Sachen auch, ja, alles.

228 A: Was müsste für dich passieren, dass du dich zum Beispiel bei Facebook abmelden
229 müsstest oder bei WhatsApp?

230 I: Ja, das ist eigentlich schwierig, weil ich sage immer auf Facebook und WhatsApp habe ich
231 keine Foto und nichts und schicke auch nichts, was mich gegebenenfalls belasten könnte.
232 Weil es gibt ja viele, die Fotos von sich herumschicken, die vielleicht nicht unbedingt für die
233 Öffentlichkeit geeignet sind. Aber das ist bei mir nicht der Fall, deswegen denke ich mir, auch
234 wenn die meine Foto haben, dann können sie mir eigentlich nichts tun, weil es ist nichts was
235 mich belasten könnte, auch von anderen Daten oder beim Schreiben und so, da ist nichts. Und
236 ansonsten würde ich mich abmelden, wenn sie monatliche Kosten verlangen oder irgendwas,

237 wo man sagt, das sind wirklich Kosten, wo du sagst, das ist es mir nicht wert, dass ich da
238 dabei bin, weil ich muss jeden Monat so und so viel bezahlen.

239 A: Nehmen wir mal an, WhatsApp und Facebook sagen, damit sie funktionieren können – ich
240 weiß jetzt nicht ob das der Fall ist – musst sie automatisch die Ton- und Videokamera ein-
241 und ausschalten können. Und nehmen wir mal an, von dir würde dann eine Aufnahme
242 gemacht, du aber weißt nicht, dass sie gemacht worden ist. Wäre das dann auch so ein Fall,
243 der zu weit geht?

244 I: Ja, in so einem Fall, nein, das geht dann schon zu weit. Weil zum Beispiel Facebook und
245 WhatsApp, das kannst du ja selbst noch kontrollieren. Zum Beispiel Facebook: ich kann
246 kontrollieren, was ich öffentlich mache, was alle sehen sollen und was nicht.

247 A: Aber im Grunde, wenn die App Zugriff auf die Fotos auf deinem Handy hat, kannst du
248 dann auch noch bestimmen welche Fotos sie nimmt oder nicht?

249 I: Zum Veröffentlichen weiß ich nicht wie das geht, ob sie diese dann auch veröffentlichen
250 kann oder nicht. Aber eigentlich, rein theoretisch nicht, weil sonst dürften sie es ja nicht
251 immer so einfach in das Internet reinstellen, wie es jetzt ist.

252 A: Kommt dann drauf an für was man die Erlaubnis erteilt hat und für was nicht.

253 I: Ja, genau.

254 A: Wie möchtest du dich in Zukunft davor schützen, dass nicht so viele Daten von dir
255 gespeichert werden?

256 I: Mich informieren vor allem. Man bekommt ja viel mit in den Medien. Ganz wichtig ist auf
257 Facebook immer wieder kontrollieren, was ist jetzt neu, auch durchlesen dann. Da nehme ich
258 mir schon oft die Zeit, das durchzulesen, wenn es neue Einstellungen gibt. Dann schau ich
259 auch, ob sich da etwas in meiner Sicherung verändert hat oder hat sich das nun alles
260 veröffentlicht, so zu sagen.

261 A: Wieso hast du ein spezielles Interesse dich zu schützen?

262 I: Ja, ich meine es muss nicht jeder alles wissen über einen selbst. Ich möchte schon selbst
263 bestimmen, was andere über mich wissen sollen und was nicht. Das hat nicht Facebook zu
264 entscheiden, was die Leute über mich wissen oder nicht.

265 A: Du hast auch gesagt in den Medien liest man viel. Hast du da spezielle Medien, die du
266 immer wieder nutzt?

267 I: Ja, da benutze ich schon auch mehr das Internet. Das ist einfach am einfachsten, das
268 Internet. Wenn du da was eingibst, gibt es viele Computerportale, weißt du, wo immer wieder
269 alles gut beschrieben ist.

270 A: Das heißt, wenn im Moment ein Thema aktuell ist, wie zum Beispiel Passwortsicherung,
271 dann liest du dir das im Internet genau durch.

272 I: Ja, genau.

273 A: Wie denkst du wird unser Leben mit dem Smartphone in 30, 50 Jahren aussehen?

274 I: Ja wir werden es überall und immer mit uns tragen, oder vielleicht eine neue Technologie
275 wird da sein.

276 A: Gut, dann haben wir den größten Teil schon durch. Jetzt sage ich dir ein paar Szenarien
277 und frage dich, ob du diese für realistisch hältst oder nicht.

278 A: Wenn jemand täglich das Smartphone mit Apps und Internet zum Beispiel Twitter
279 und/oder Facebook nützt, ohne jedoch jemals seinen Standort preiszugeben. Wäre es für dich
280 dann vorstellbar, dass man mit großer Wahrscheinlichkeit vorhersagen kann, wo sich
281 derjenige in Zukunft aufhalten wird?

282 I: Ja ich denke schon, dass das irgendwie möglich ist.

283 A: Wieso?

284 I: Auch wenn man seinen Standort nicht preisgibt, orten kann man ein Handy immer, weißt
285 du. Man kann es ja doch orten, auch wenn man den Standort nicht preisgibt. Also du bist doch
286 immer im Netzwerk vertreten, deshalb.

287 A: Und wenn wir jetzt annehmen, der Max verliert sein Handy, kannst du dir vorstellen, dass
288 man nur durch ein paar enge Freunde auf Facebook sich ausrechnen kann, wo der ungefähr
289 ist, auch wenn der Max kein Handy hat, das man irgendwie orten könnte und auch nicht jetzt
290 jemand zum Beispiel postet, der Max ist mit mir dort oder Fotos reinstellt oder so. Einfach
291 nur mit Standortdaten von den Freunden, dass man dann rausfinden kann, der Max ist dort.

292 I: Irgendeine Möglichkeit, ich sage möglich ist es sicher, irgendwie immer. Ich könnte das
293 jetzt nicht. Also wenn ich das jetzt rausfinden möchte, ich würde das nicht können, aber ich
294 glaube es gibt da intelligente Menschen, die das immer rausfinden.

295 A: Hast du schon einmal davon gehört?

296 I: Ja, ich habe schon mal etwas davon gehört, dass das möglich ist. Jetzt genau in dem Fall
297 nicht, aber wenn jemand, vor allem, wenn jemand aktiv ist auf Facebook oder so, dann findet
298 man das leicht raus eigentlich.

299 A: Wie realistisch ist es für dich, dass die Polizei bereits heute wissen kann, wo morgen ein
300 Verbrechen stattfindet? Nehmen wir jetzt nicht unbedingt Ort 1 her, sondern eine größere
301 Stadt, wo mehr Verbrechen stattfinden.

302 I: Ja, realistisch ist es schon. Vor allem, wenn sie ein paar Menschen beobachten, weil sie
303 glauben, die haben was im Schilde. Die Polizei kann ja jederzeit abhören, die können ja

304 jederzeit kontrollieren, ob du telefonierst oder schreibst. Deshalb glaube ich schon, dass das
305 möglich ist.

306 A: Könntest du dir vorstellen, dass auch, wenn es jetzt keine Bande gibt, wo man weiß, ok die
307 überwachen wir, sondern rein von früheren Verbrechen und deren Standorte, dass man sich
308 ausrechnen kann, das nächste wird dort wahrscheinlich stattfinden.

309 I: Ja. Nehmen wir an, da muss man sich dann aber schon dahinter setzen. Ich sage, da braucht
310 man ein paar, wo man glaubt, dass die was im Schilde führen. Wenn du nicht weißt, wer
311 dieses Verbrechen machen könnte, so zu sagen, dann hast du eigentlich, dann müsstest du alle
312 Personen abhören, das ist unrealistisch.

313 A: Hast du schon einmal davon gehört?

314 I: Dass sie das voraussagen können?

315 A: Ja.

316 I: Nein.

317 A: Nehmen wir an, eine Frau kauft im Supermarkt verschiedene Sachen ein, jedoch keinerlei
318 Babysachen. Kannst du dir vorstellen, dass man nur aus den gekauften Artikeln mit hoher
319 Wahrscheinlichkeit sagen kann, ob diese Frau schwanger ist oder nicht und ungefähr auch den
320 Geburtstermin feststellen kann?

321 I: Also wenn man das über längere Zeit beobachtet 100-prozentig. Also jetzt vielleicht nicht
322 genau welches Monat, das ist vielleicht schätzungsweise.

323 A: Wieso kann man das generell herausfinden?

324 I: Also ich glaube, wenn man schwanger ist, dann kauft man andere Produkte ein, die man
325 sonst vielleicht im alltäglichen Leben nicht einkaufen würde. Außer es sind wirklich ein paar,
326 die immer gleich leben. Aber halt ich glaube schon, dass, wenn man das genau beobachtet,
327 dass man das dann auch sieht.

328 A: Wieso den Geburtstermin nicht unbedingt?

329 I: Ja, da muss man schon gut im Schätzen sein. Sieht man die Frau immer?

330 A: Nein, nur das, was eingekauft wird.

331 I: Ja, man kann vielleicht sehen dass es langsam, langsam soweit ist, aber nicht genau den
332 Termin.

333 A: Nein, jetzt genau den Termin nicht, aber dass man sieht frühe Schwangerschaft, mittel
334 oder Ende.

335 I: Das denke sieht man sicher am Einkaufswagen, weil man doch Produkte kauft, die man
336 dann braucht, wenn man im achten oder neunten Monat schwanger ist, die man vorher noch
337 nicht gebraucht hat.

338 A: Hast du schon einmal davon gehört?

339 I: Nein.

340 A: Nehmen wir an, ein Mann ist homosexuell, er nützt das Internet, darunter auch Social
341 Media, gibt jedoch nirgends an, dass er Männer liebt. Sein Sexualleben wird also von ihm
342 nicht preisgegeben - weder im Internet, noch sonst irgendwo. Für wie realistisch haltest du es,
343 dass wildfremde Personen dennoch mit hoher Wahrscheinlichkeit sagen können, dass Max
344 homosexuell ist?

345 I: Ja, ich glaube, naja ich weiß nicht ob das so. Weil oft meint man, dass ein Mann
346 homosexuell ist, ist es aber dann gar nicht. Manchmal hat man Vorurteile gegen jemanden,
347 wo man das auch nicht wirklich einschätzen kann.

348 A: Aber mit einer gewissen Wahrscheinlichkeit kannst du dir vorstellen, dass man das sagen
349 kann, es gibt dann ja immer noch die restlichen Prozent.

350 I: Ja, ich sage mal mit 60, 70 Prozent, kann man das sagen. Man sieht das ja auch bei der
351 Person, wie sie sich gibt, wie sie sich kleidet. Vielleicht könnte man es schon. Wenn man
352 diese länger beobachtet, er muss auch nicht viel preisgeben, aber wenn man diesen länger
353 beobachtet, dann kann man das wahrscheinlich schon herausfinden.

354 A: Wieso sieht man das zum Beispiel beim Anziehen oder beim Verhalten.

355 I: Ich weiß auch nicht, mir kommt vor sie verhalten sich oft ein wenig anders, weil sie einfach
356 eine andere Einstellung haben. Nicht alle, aber einzelne.

357 A: Hast du schon einmal davon gehört?

358 I: Ja, kann man schon sagen.

359 A: Oder selbst erlebt?

360 I: Ma, selbst erlebt. Ja, selbst erlebt, ich habe mir halt gedacht, bei jemandem, dass der
361 homosexuell sein könnte, aber ich habe das nie behauptet, dass er das wäre, aber es hat sich
362 dann im Grunde schon so herausgestellt, dass er das ist.

363 A: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft deine Freundesliste auf Facebook
364 kontrollieren und auch die Bewegungsdaten von deinem Smartphone heranziehen, wenn sie
365 prüfen wollen, ob du überhaupt eine Kredit bekommst oder nicht?

366 I: Ja, möglich. Ich sage schon.

367 A: Wieso?

368 I: Um zu schauen, in welchen Kreisen du unterwegs bist und einfach auch zu schauen, welche
369 Tätigkeit du ausführst.

370 A: Was sagt das aus dann?

371 I: Ja, die ganze Lebenseinstellung, zum Beispiel.

372 A: Hast du schon einmal davon gehört?

373 I: Nein, gehört nicht.

374 A: Kennst du die Gesundheits- und Fitness-App's, die man am Smartphone herunterladen
375 kann?

376 I: Ja.

377 A: Kannst du dir vorstellen, dass in Zukunft sich Gesundheitsversicherungen mit solchen
378 Apps zusammenschließen, wenn sie überprüfen wollen, ob du regelmäßig Sport machst und
379 ob du dich gesund ernährst, und entscheiden, ob du eine Versicherung bekommst oder nicht
380 und welche?

381 I: Möglich sage ich mal, ist alles. Sicher ist es für die Versicherung ein Vorteil, weil wenn sie
382 sehen, ich bin aktiv und alles, weil sie sehen ja im Grunde was ich mache mit diesem App und
383 dann vielleicht können sie das schon etwas einschätzen, weil wenn ich nur bei ihnen sitze und
384 ihnen was erzähle, dann können sie das ja nicht kontrollieren. Und mit der App haben sie
385 vielleicht ein bisschen eine bessere Kontrolle über mich.

386 A: Dass sie sich dann absichern auch?

387 I: Genau.

388 A: Hast du schon einmal davon gehört?

389 I: Nein.

390 A: Für wie wahrscheinlich hältst du das Szenario, dass man in Zukunft in ein Land nicht mehr
391 einreisen darf, weil man zum Beispiel ein bestimmtes Wort im Internet eingegeben hat, auf
392 Google gesucht hat oder in einer SMS etwas geschrieben hat, was nicht gut ist. Jetzt sage ich
393 mal eine SMS geschrieben hat mit: wir werden Amerika zerstören, zum Beispiel.

394 I: Ich glaube das ist unrealistisch in diesem Fall. Ich hoffe, dass es nicht so weit kommen
395 wird, weil wenn es mal soweit ist, dann muss man sich echt Gedanken machen.

396 A: Ok. Wieso hältst du es für unrealistisch?

397 I: Ja, ich weiß nicht, da bräuchte es schon viele Leute, die das jeden Tag kontrollieren. Da
398 muss ja rein theoretisch eine Person ein paar Personen überprüfen und immer schauen, was
399 diese geredet und geschrieben haben.

400 A: Könntest du dir das mit der Technik gar nicht vorstellen?

401 I: Ja gut, wenn es ein Computer übernimmt. Sagen wir so, wenn es ein Computer übernimmt,
402 dann muss man sich immer in einer Standardsprache ausdrücken, aber wenn man in Dialekt
403 schreibt oder so würde er es dann nicht verstehen.

404 A: Also einzelne Wörter würde er dann nicht erkennen. Weil zerstören klingt wohl
405 standardmäßig.

406 I: Ja das schon, in dem Fall schon, aber vielleicht sonst andere einzelne Wörter, wenn man die
407 umändert in einen Dialekt, den der Computer nicht erkennen kann, dann ...

408 A: Dann glaubst du, dass der Dialekt gar nicht im Computer gespeichert ist?

409 I: Nein.

410 A: Was ist zum Beispiel, wenn jemand im Internet „Bombe“ sucht. Wäre das ein Grund,
411 warum derjenige nicht mehr einreisen darf oder die Einreise sehr erschwert wird?

412 I: Ja, ok, das ist schon ein Grund, dass die Einreise erschwert wird, weil wenn ich mich mit
413 dem Thema auseinandersetze, Bombe, dann interessiere ich mich in diesem Fall ja für das.
414 Aber ich glaube, das muss man hinterfragen, wozu das gesucht worden ist, weil ich kann ja
415 auch nur das Interesse haben oder wegen einem Referat oder weil ich gedacht habe, ich muss
416 das nachforschen, wie funktioniert das eigentlich. Das weiß man ja eigentlich nicht.

417 A: Denkst du dann, das wird nachgeforscht oder wird einfach kurzer Prozess gemacht und die
418 Einreise verweigert.

419 I: Nein ich denke schon, dass nachgeforscht wird. Ich hoffe zumindest, dass nachgeforscht
420 wird.

421 A: Hast du schon einmal davon gehört?

422 I: Nein.

423 A: Ist es für dich realistisch, dass man aus dem Verhalten der Vergangenheit, das Verhalten in
424 der Zukunft schon vorhersagen kann?

425 I: Teils, teils sage ich. Weil nur, weil ich mich in der Vergangenheit so verhalten habe, muss
426 das nicht heißen, dass ich mich in der Zukunft auch so verhalten muss. Also man macht ja
427 verschiedene Phasen durch in seinem Leben und man verändert sich ja auch, nur weil man
428 vielleicht - ich sage mal, ich war früher ein Rebell, hat alles zerstört, keine Ahnung, weiß ich
429 ja nicht, aber das heißt ja nicht, dass ich das ein Leben lang sein muss. Es kann ja auch etwas
430 passiert sein, durch eine Arbeitsstelle oder durch eine Person, durch das ich mich geändert
431 habe und jetzt eine komplett andere Person in der Zukunft bin.

432 A: Könntest du dir auch vorstellen, dass man zum Beispiel schon heute sagen kann ok: Wenn
433 sie sich in der Kindheit oder als Jugendlicher so verhalten und sich nachher dann entweder in
434 eine positive oder negative Richtung entwickeln oder wenn sie gleich arbeiten gehen oder
435 studieren, dann ist die Wahrscheinlichkeit groß, dass sie sich danach entweder normal
436 verhalten oder sehr stark rebellieren, oder sehr aktiv oder sehr erfolgreich. Meinst du kann
437 man das irgendwie schon vorhersagen, ok, wenn das so eintritt, dann ist die
438 Wahrscheinlichkeit hoch, dass derjenige dann studieren geht oder dass der erfolgreich wird.
439 Dass man das schon ein bisschen einschätzen kann?

440 I: Bei ein paar Sachen sicher. Zum Beispiel wenn ein Kind relativ alleine, ohne Eltern
441 aufgewachsen ist oder die Eltern schon kriminell waren und nachlässig waren und er das nie
442 anders vorgezeigt bekommt, dann kann es schon sein, dass die Wahrscheinlichkeit groß ist,
443 dass er auch in diese Fußstapfen reintritt, dass ihm nichts wichtig ist, die Schule ist nicht
444 wichtig, die Arbeit ist nicht wichtig, weil einfach die Vorbilder, die Eltern, ihm das so
445 vorgelebt haben. Da kann es schon sein, dass die Wahrscheinlichkeit hoch ist, dass er sich so
446 entwickelt. Das gleiche ist auch, wenn du schon erfolgreiche Eltern hast, dann ist es leichter
447 für dich, auch erfolgreich zu sein, sagen wir so. Es muss nicht sein, aber du hast schon was,
448 dir ist schon was gegeben, du hast schon was, worauf du aufbauen kannst auch, dann denke
449 ich mir ist die Wahrscheinlichkeit groß, dass das bei dir auch in diese Richtung gehen kann.

450 A: Hast du das bei deiner Ausbildung gelernt oder irgendwann mal gelesen oder gehört, dass
451 das so sein könnte?

452 I: Ja in der Schule hat man schon auch oft Fälle von dem gehört, dass das so sein kann.

453 A: Jetzt als Lehrbeispiel oder dass Mitschüler das erlebt haben.

454 I: Als Diskussionsform, sagen wir so, haben wir das gemacht.

455 A: Wo du dann wirklich auch solche Fälle von der Praxis her kennst oder mehr nur als
456 Theorie?

457 I: Alles nur Theorie, also persönlich kannte ich da keinen.

458 A: Gut, danke für das Interview.

1 **Interview 9, am 28.10.2014. Dauer 25:29 Minuten**
2
3 A: Wie alt bist du, und was machst du beruflich?
4 I: Ich bin 24 und arbeite für Firma 2.
5 A: Mit welchen Medien informierst du dich vorwiegend?
6 I: Meinst du überhaupt?
7 A: Ja.
8 I: Fernsehen hauptsächlich, Internet.
9 A: Schaust du da auch Nachrichten, speziell?
10 I: Eigentlich nicht, das was man halt im Fernsehen und Radio hört. Also Radio auch.
11 A: Was schaust du beim Internet?
12 I: Stol wenn, aber das sehr selten. Also hauptsächlich Radio und Fernsehen.
13 A: Und sonst im Internet? Benützt du Facebook?
14 I: Facebook, Twitter, Instagram, alles mögliche.
15 A: Zeitung oder so was?
16 I: Nicht viel, eigentlich fast nie.
17 A: Nützt du Apps täglich?
18 I: Ja, eigentlich schon.
19 A: Welches Smartphone besitzt du?
20 I: Marke 1. Model 1.
21 A: Für was gebrauchst du dein Smartphone?
22 I: Internet, generell. Ich nutze es für die Arbeit. Facebook, Instagram, Twitter, und so weiter. Bilder.
23 A: Das heißt Fotos machen?
24 I: Ja.
25 A: Telefonieren, SMS schreiben?
26 I: Telefonieren, ja logisch, SMS, WhatsApp.
27 A: Wecker?
28 I: Auch.
29 A: Hast du auch Apps auf dein Smartphone heruntergeladen?
30 I: Ja, Terminkalender zum Beispiel.
31 A: Hast du dir runtergeladen?
32 I: Ja, weil der Google-Kalender synchronisiert mit allem.
33 A: Mit GMail meinst du dann?
34 I: Ja, genau. Was hab ich denn dann noch? Verschiedene Internetbrowser, Musik hören.

35 A: Da hast du dir immer Apps heruntergeladen?
36 I: Viele, ja.
37 A: Was sind dann deine Apps, die du heruntergeladen hast?
38 I: Google-Kalender, von den Browsern Opera, Chrome, Facebook-App, Twitter-App,
39 Instagram-App, WhatsApp. Was habe ich denn noch, da muss ich nachschauen.
40 A: Wetter-App vielleicht?
41 I: Ja, Wetter-App.
42 A: Taschenlampe?
43 I: Auch. Outlook-App um die E-Mails zu verwalten. YouTube, Intervalltrainer, Navi, Adobe
44 Reader, Fernbedienung für den Computer, und Notizen zu machen, Übersetzer-App, Shazam
45 App, wo man Lieder erkennen kann.
46 A: Wie oft verwendest du diese Apps?
47 I: Täglich.
48 A: Alle?
49 I: Schon eigentlich.
50 A: Hast du schon einmal den Begriff Big Data gehört?
51 I: Nein.
52 A: Hast du dennoch eine Vorstellung, was man darunter verstehen könnte?
53 I: Großes Datenvolumen, so was.
54 A: Datenschutz ist dir das ein Begriff?
55 I: Ja.
56 A: Wie gut kennst du dich mit Datenschutz aus?
57 I: Eigentlich nicht gut, ich meine man hört es oft, man hört es auch in den Nachrichten, dass
58 das nicht so geheuer abläuft, oder?
59 A: Ja, nicht immer alles reibungslos. Wenn du jetzt jemandem erklären müsstest, was
60 Datenschutz ist, was würdest du dann sagen?
61 I: Wenn du dich irgendwo anmeldest, dass die Daten nicht an die Öffentlichkeit gelangen,
62 deine persönlichen Daten.
63 A: Wenn du sagst irgendwo anmelden, ist das dann offline und online oder nur eines von
64 beiden?
65 I: Sagen wir registrieren, wenn du dich irgendwo registrierst, dass die Daten dann nur auf
66 dieser Seite bleiben, nicht auf andere.
67 A: Das heißt jetzt, es ist nur auf das Internet bezogen?
68 I: Nein, sonst auch, dass diese nicht weitergegeben werden.

69 A: Hast du den Begriff Datenschutzrichtlinie schon mal gehört?
70 I: Ja.
71 A: Was meinst du steht in einer Datenschutzrichtlinie drinnen?
72 I: Das, was ich gerade gesagt habe.
73 A: Könntest du das bitte noch einmal kurz zusammenfassen?
74 I: Dass, wenn man sich bei einer gewissen Seite registriert, dass meine persönlichen Daten
75 nur auf dieser Seite bleiben und nicht in die Öffentlichkeit gelangen.
76 A: Das heißt aber, dass sie an andere schon weitergegeben werden dürfen?
77 I: An andere Seiten?
78 A: An andere Seiten, oder andere Firmen oder an Dritte oder so?
79 I: Nein, dass sie nur auf dieser Seite bleiben.
80 A: Ok, aber diese Seite oder diese Firma darf mit diesen Daten alles tun. Sie darf sie zwar
81 nicht an die Öffentlichkeit geben, oder an Dritte, aber sie selbst dürfen damit alles machen,
82 was sie gerne machen würden?
83 I: Das wäre zum Beispiel?
84 A: Zum Beispiel speichern, analysieren, für Programme verwenden.
85 I: Das weiß ich jetzt nicht, aber ich denke mir, das sollten sie eigentlich nicht. Ich glaube
86 nicht. Also, dass sie gespeichert werden, das schon, bei der Registration. Aber, dass sie
87 machen dürfen, was sie wollen, das nicht.
88 A: Hast du dir schon mal eine Datenschutzrichtlinie durchgelesen?
89 I: Nein.
90 A: Hast du bereits einmal eine Datenschutzrichtlinie unterzeichnet oder akzeptiert?
91 I: Akzeptiert sicher.
92 A: Weißt du noch wo das war?
93 I: Weiß ich nicht mehr.
94 A: Wenn wir nun an deine Apps denken: Meinst du, haben deine Apps eigene
95 Datenschutzrichtlinien?
96 I: Ja, es werden halt gewisse Richtlinien vorgegeben sein, aber auf die App angepasst
97 vielleicht.
98 A: Wo kann man sich über diese Datenschutzrichtlinie z.B. von Apps informieren?
99 I: Bei der App selbst.
100 A: Weißt du da wo genau?
101 I: Nein, keine Ahnung, über die App vielleicht. Bei den Einstellungen.

102 A: Wenn du jetzt sagst bei der Registration speichert die Firma die Daten. Das heißt, wenn du
103 jetzt eine App installierst, kann diese dann schon, hat sie dann Zugriff auf deine Daten?

104 I: Nein, ich denke das ist nur eine Übersicht für die Firma, dass diese gewisse Person die App
105 schon heruntergeladen hat.

106 A: Was verstehst du alles unter Daten? Was fällt da alles rein?

107 I: Ma, Name, Geburtsdatum, E-Mail-Adresse vielleicht.

108 A: Also hat die App auf diese Daten Zugriff, so zu sagen?

109 I: (...?) Ja.

110 A: Sonst noch irgendwas? Kannst du dir noch etwas vorstellen, worauf die App Zugriff hat,
111 wenn sie Zugriff hat.

112 I: Kommt drauf an, was du angibst. Ich meine die Pflichtfelder sind eh diese, die ich dir
113 angesagt habe.

114 A: Kannst du dir auch vorstellen, dass die App Zugriff auf die Fotos hat, die Videokamera,
115 den Kalender, Adressbuch?

116 I: Facebook sicher. Facebook sieht sicher alle Fotos und Infos, die du hast. Vielleicht auch die
117 Chats selbst auch, wird es auch sehen, denke ich mir.

118 A: Aber sieht Facebook, dann praktisch nur die Fotos, die du auf dem Account drauf hast,
119 oder sieht Facebook, hat Facebook auch die Möglichkeit von deinem Handy, was du nicht auf
120 Facebook gepostet oder gespeichert hast, auch auf deinem Smartphone die Fotos anzusehen,
121 die du privat gemacht hast, ohne sie mit Facebook zu verbinden?

122 I: Ich denke schon.

123 A: Wieso?

124 I: Ja weil, wenn du ein Foto auswählst für Facebook, dann siehst du da ja auch schon alle,
125 obwohl du sie nicht raufgeladen hast.

126 A: Jetzt sage ich dir ein Szenario. Du machst ja Fotos mit deinem Handy, hast du gesagt.
127 Richtig?

128 I: Ja.

129 A: Angenommen, der Max benützt sein Handy immer nur zu Hause und alleine, ohne, dass
130 sich jemand anderer neben ihm oder im gleichen Raum aufhält. Glaubst du, ist es dann
131 dennoch möglich, dass irgendjemand seine Fotos sehen kann, ohne dass er es ihnen zeigt oder
132 schickt?

133 I: Ja, durch eben solche Apps.

134 A: Ist es für dich realistisch, dass es dem Max gar nicht bewusst ist, dass andere seine Fotos
135 sehen können?

136 I: Ja.
137 A: Das funktioniert dann auch wieder mit den Apps?
138 I: Ja.
139 A: Wieso ist ihm das, meinst du, nicht bewusst?
140 I: Ja, ich weiß nicht, aber vielleicht, weil man nie soweit denkt, wenn man so eine App
141 installiert. Oder, dass man von dem gar nicht ausgeht.
142 A: Wie gut sind deine Fotos vor der Einsichtnahme anderer Personen geschützt, zum Beispiel
143 auf deinem Smartphone?
144 I: Also auf dem Handy selbst, da habe ich auch einen Sicherheitscode oder ein Muster, dass
145 man überhaupt nichts sieht, aber durch die Apps eigentlich haben dann doch wieder viele
146 Zugriff, eigentlich schon.
147 A: Wer bestimmt die Sicherheit von deinen Daten auf deinem Handy?
148 I: Was ist unter Sicherheit gemeint?
149 A: Wer sagt, dass diesen Inhalt der und der sehen darf, oder gar niemand oder nur bestimmte
150 Personen?
151 I: Jetzt auf die Facebook-App bezogen, kannst du das auswählen, wer was sieht, ob es
152 Freunde sehen oder Freundesfreunde. Aber ich denke Facebook selbst, ist das egal, was du
153 angibst. Sie sehen trotzdem alles.
154 A: Kannst du das irgendwie regeln? In Facebook ist das wieder eine andere Geschichte, aber
155 die Facebook-App darf zum Beispiel keinen Zugriff haben auf meine Fotos. Oder die
156 Taschenlampen- und Wetter-App dürfen keinen Zugriff auf meine Fotos haben. Kannst du
157 das regeln selbst?
158 I: Wüsste ich nicht, ob ich das regeln könnte.
159 A: Ok. Kannst du das irgendwie überprüfen, ob eine App Zugriff auf einen Bereich hat?
160 I: Nein.
161 A: Die App, hast du gesagt, bekommt diesen Zugriff durch die Datenschutzrichtlinien, wenn
162 wir diese akzeptieren. Wieso meinst du, braucht eine Wetter-App Zugriff auf verschiedene
163 Bereiche? Weil du kannst dir wahrscheinlich vorstellen, dass die Wetter-App Zugriff auf das
164 Internet braucht, um funktionieren zu können, aber wieso meinst du schreibt die Wetter-App
165 in die Datenschutzrichtlinien rein, dass sie Zugriff auf das Adressbuch, die Fotos, den
166 Kalender braucht.
167 I: Ja du kannst das Wetter ja auf deinen eigenen Standort aktualisieren. Dass sie Zugriff haben
168 auf dein GPS vielleicht, damit sie sehen können wo du bist und dir dann das Wetter ansagen
169 können.

170 A: Das ist sicher einmal. Kannst du dir auch beim Adressbuch eine Funktion dafür vorstellen?
171 Oder wieso braucht sie diesen Zugriff?

172 I: Keine Ahnung, vielleicht wenn du so eine Schnellfunktion hast, wo du eingeben kannst
173 Standort Zuhause, dass sie dann gleich wissen, was gemeint ist.

174 A: Ok, dass du das gekoppelt hast.

175 I: Ja.

176 A: Gibt es noch andere Gründe, wieso das die App benötigen könnte?

177 I: Nein. Außer du machst was mit der App, was du nicht darfst, damit sie dich gleich finden
178 können.

179 A: Ja, das ist dann wieder eine andere Sache. Das heißt, eigentlich die Apps speichern diese
180 Informationen irgendwo?

181 I: Ich denke schon.

182 A: Und wieso werden diese Daten gespeichert oder diese Foto, Nummern usw.? Wer könnte
183 daran interessiert sein?

184 I: Die, wie heißt sie nochmal? Die NSA.

185 A: Die Geheimdienste.

186 I: Ja, genau.

187 A: Welchen Grund haben die Geheimdienste überhaupt Daten zu speichern?

188 I: Keine Ahnung, wenn jemanden das nicht bewusst ist, das die darauf Zugriff haben, dann
189 könnte man ja, ganz krass gesagt, über Facebook was planen und aushacken. Dass sie
190 dahinter kommen.

191 A: Praktisch Kontrolle?

192 I: Ja.

193 A: Was meinst du können jetzt Geheimdienste wie die NSA, aber auch andere Unternehmen,
194 die ganz viele Daten haben, sagen wir mal eine Firma von einer App, die unzählig viele Daten
195 von ganz, ganz vielen Leuten haben. Was können sie mit diesen Daten anfangen? Welchen
196 Vorteil bringen ihnen diese vielen Daten?

197 I: Überprüfung.

198 A: Von was?

199 I: Wie viele registriert sind. Wo vielleicht. Wo auf der Welt, dass mehr registriert sind.
200 Altersgruppen.

201 A: Können sie dann irgendwas daraus schließen?

202 I: Ja, eigentlich schon. Keine Ahnung, wenn es nur junge Leute nehmen, dann wird es für
203 ältere wohl zu kompliziert sein oder weißt du, so Schlussfolgerungen halt von den vielen
204 Daten.

205 A: Dass sie das dann an jemanden anpassen können?

206 I: Ganz genau.

207 A: Das sind im Grunde die Vorteile auf der einen Seite für das Unternehmen. Kann das für
208 uns auch Vor- oder Nachteile haben?

209 I: Ja, keine Ahnung, dass die App angepasst wird, vielleicht.

210 A: Ja, das ist ein Vorteil für uns. Gibt es auch Nachteile?

211 I: Ja, die haben halt immer die Daten von dir.

212 A: Das heißt du kannst überprüft werden?

213 I: Ja. Genau. Also die Privatsphäre ist dahin. Also auf ein Minimum reduziert.

214 A: Ist das für dich jetzt ein Punkt, der dich stört? Ist dir das wichtig?

215 I: Ich mache nichts, was ich nicht darf, deshalb ist mir das eigentlich egal, aber es ist halt
216 nicht angenehm zu wissen, dass man bei allem, was man macht, überprüft werden könnte.

217 A: Hast du dir schon mal überlegt, einen Dienst oder eine App deswegen zu löschen?

218 I: Nein, eigentlich nicht. Solange alles so geschieht, dass ich ok bin, ist mir das eigentlich
219 gleich.

220 A: Was müsste passieren, dass du sagst, das geht jetzt eindeutig zu weit, ich lasse das jetzt?

221 I: Wenn die Daten irgendwie veröffentlicht werden, ohne dass ich es weiß oder ohne, dass ich
222 dem zugestimmt habe. Und die Daten werden dennoch veröffentlicht.

223 A: Ja. Was wäre jetzt zum Beispiel, wenn du eine Taschenlampen App herunterladest und bei
224 der Installation erlaubst, dass sie zum Beispiel Zugriff hat auf das Tonband, dass sie auch
225 automatisch ein- und ausschalten kann, und dass sie auch Zugriff auf das Internet erhält und
226 sie jetzt zum Beispiel in einer Situation, in der du nicht möchtest, dass das jemand anderes
227 erfährt, das Tonband einschaltet und eine Audioaufnahme macht und diese nachher
228 veröffentlicht. Wäre das dann etwas, wo du sagst, das geht zu weit? Weil eigentlich hast du ja
229 zugestimmt, dass sie das machen darf und dass sie diese Daten verwenden darf.

230 I: Ja. Das schon.

231 A: Wie möchtest du dich in Zukunft vor Datenraub oder –Speicherung schützen?

232 I: Vielleicht die Datenschutzrichtlinien genau durchlesen.

233 A: Mhm. Ok. Dass du auch weißt, wo du zustimmst.

234 I: Ja.

235 A: Wie denkst du wird unser Leben mit dem Smartphone in 30, 50 Jahren aussehen?

236 I: Ja es werden noch mehr Technologien in unseren Alltag eingebaut.

237 A: Gut, dann haben wir den größten Teil unseres Interviews hinter uns. Ich schildere dir nun

238 ein paar Szenarien und frage dich, ob du diese für realistisch hältst oder nicht und warum.

239 Wenn jemand täglich das Smartphone mit Apps und Internet zum Beispiel Twitter und/oder

240 Facebook nutzt, aber jedoch niemals seinen Standort preisgibt, wäre es für dich dann

241 vorstellbar, dass man mit großer Wahrscheinlichkeit vorhersagen kann, wo sich diese Person

242 in Zukunft aufhalten wird?

243 I: In Zukunft?

244 A: Mhm.

245 I: Kann sein. Ja, eigentlich schon.

246 A: Warum?

247 I: Ja, vielleicht, wenn das lange verfolgt wird, dass wenn, keine Ahnung, wenn einer sich

248 immer ungefähr im gleichen Raum aufhält, das man dann das ungefähr auf eine gewisse

249 Fläche begrenzen kann.

250 A: Mhm, dass man dann weiß, an diesen Punkten ist er vor allem. Kannst du dir auch

251 vorstellen, dass man zum Beispiel nur durch ein paar Standorte von ein paar Facebook-

252 Freunden sich das auch ausrechnen kann, wo er sich aufhält?

253 I: Ja!

254 A: Wieso?

255 I: Durch den Chat.

256 A: Ok, nehmen wir mal an diese Person X ist gar nicht daran beteiligt, weder in Chats noch

257 werden Fotos mit dieser Person gepostet und keine Post mit den Standortangaben dieser

258 Person gemacht. Könntest du dir dann auch vorstellen, dass auch, wenn man nur den Standort

259 von diesen Facebook-Freunden hat, dass man dann rein mit diesen Angaben mit hoher

260 Wahrscheinlichkeit den Standort der betreffenden Person ausrechnen kann?

261 I: Ohne dass miteinander geschrieben wird?

262 A: Ja, ohne dass geschrieben wird.

263 I: Die Wahrscheinlichkeit könnte sich wahrscheinlich erhöhen, wenn du in der Vergangenheit

264 öfters mit ihnen unterwegs warst.

265 A: Ja, wieso das?

266 I: Ja, weil wenn du in der Vergangenheit öfters mit ihnen unterwegs warst, dann ist es gut

267 möglich, dass du heute auch mit ihnen unterwegs bist, wenn du viel mit ihnen unterwegs

268 warst.

269 A: Das heißt, dass man das mit einer Statistik berechnen kann?

270 I: Ja, genau.

271 A: Hast du schon davon einmal gehört?

272 I: Ich hab mir schon manchmal Gedanken gemacht, aber nicht genau auf das bezogen, mehr
273 von anderen Sachen.

274 A: Über was hast du da nachgedacht?

275 I: Bezüglich Abhören von Telefonaten usw. oder dass sie sogar Zugriff auf die Kamera
276 haben.

277 A: Hat das mit dem NSA-Skandal auch ein bisschen zu tun?

278 I: Auch, ja.

279 A: Wie realistisch ist es für dich, dass die Polizei bereits heute wissen kann, wo morgen ein
280 Verbrechen stattfindet?

281 I: Wichtig schon, aber wenn es so rausgefunden wird, dass man dann bei allem überwacht
282 wird. Ja ich mein, jetzt bei einem Verbrechen, das groß geplant wird, ist es vielleicht ein
283 Vorteil, aber wie gesagt, es ist nicht fein, dass man weiß, dass man bei allem, was man tut,
284 überwacht wird.

285 A: Aber ist es für dich realistisch, dass die Polizei das vorhersagen kann?

286 I: Ja!

287 A: Wie funktioniert das dann?

288 I: Keine Ahnung, auch vielleicht indem sie Telefonate abhören usw. Wenn sie rausfinden,
289 dass etwas geplant ist.

290 A: Kannst du dir vorstellen, dass auch, wenn sie jetzt keinen direkten Hinweis haben oder
291 keine Spur, die sie verfolgen, sondern nur die Verbrechen der Vergangenheit, dort die
292 Standorte zusammentragen und dann schon sagen können, relativ genau, dass morgen mit
293 einer Wahrscheinlichkeit von 20% dort etwas passiert, mit einer Wahrscheinlichkeit von 40%
294 da usw.

295 I: Ja, kann schon sein, wenn irgendein Muster dahinter ist bei den vielen Standorten, das
296 vielleicht.

297 A: Hast du schon einmal davon gehört?

298 I: Nein.

299 A: Nehmen wir an, eine Frau kauft im Supermarkt verschiedene Sachen ein, darunter aber
300 keinerlei Babysachen. Kannst du dir vorstellen, dass man nur aus den gekauften Artikeln mit
301 hoher Wahrscheinlichkeit sagen kann, ob diese Frau schwanger oder nicht?

302 I: Ja.

303 A: Wieso?

304 I: Ja, weil Schwangere nicht alles essen können, was sie vielleicht wollen, sondern dass sie
305 auf gewisse Sachen schauen müssen.

306 A: Dass sie das Einkaufsverhalten ändern?

307 I: Ja. Ja.

308 A: Kannst du dir auch vorstellen, dass man schon relativ genau den Geburtstermin, oder sagen
309 wir Anfang der Schwangerschaft, Mitte und Ende der Schwangerschaft, auch das bestimmen
310 kann?

311 I: Ich weiß nicht genau, was eine Frau isst am Ende der Schwangerschaft gegenüber dem
312 Anfang der Schwangerschaft. Aber wenn sich das ändert, dann schon. Wenn es typische
313 Sachen gibt, die man eher am Ende isst, dann kann man das leicht herausfinden.

314 A: Hast du schon einmal davon gehört?

315 I: Nein.

316 A: Nehmen wir an, ein Mann ist homosexuell, er nützt das Internet, darunter auch Social
317 Media, gibt aber nirgends an, dass er Männer liebt. Er hält sein Sexualleben auch geheim, gibt
318 es also nirgends an - weder im Internet, noch sonst irgendwo. Für wie realistisch hältst du es,
319 dass wildfremde Personen dennoch mit hoher Wahrscheinlichkeit sagen können, dass der
320 Mann homosexuell ist?

321 I: Realistisch schon, keine Ahnung.

322 A: Gibt es einen Grund dafür?

323 I: Er wird wohl doch mit Leuten zu tun haben, wenn er das ist, oder vielleicht hat er dann mit
324 dem einen nichts mehr zu tun und der erzählt das dann weiter. So halt.

325 A: Ok, dass das dann weitergesagt wird. Wenn das jetzt nicht weitererzählt wird und ihn eine
326 Person sagen wir mal, ihn ein bisschen kontrolliert, kann man das dann auch herausfinden?

327 I: Hm. Kann, sein, ja.

328 A: Wusstest du da, wie das geht?

329 I: Ja, ich weiß nicht. Er wird wohl, wenn er homosexuell ist mit jemandem zu tun haben,
330 vielleicht ist er in einer Beziehung oder was weiß denn ich. Und wenn die dann nicht mehr
331 klappt, dass dann vielleicht der Ex-Partner das einer Person erzählt und die erzählt es dann
332 einer anderen.

333 A: Ok, aber rein von den Verhaltensweisen kann man das nicht unbedingt herausfinden, mehr
334 wird es nur weitererzählt?

335 I: Entweder das, oder es kennt sich jemand sehr gut aus mit dem menschlichen Verhalten.
336 Zum Beispiel, dass er die typischen Gesten lesen kann, das vielleicht.

337 A: Wäre es für dich auch vorstellbar, dass wenn es zum Beispiel so wäre, dass zum Beispiel
338 sehr viele homosexuelle Männer einen gelben Pullover besitzen und jemand kauft einen
339 gelben Pullover, dass er dann automatisch auch mit einem gewissen Prozentsatz dazugehört?
340 I: Es kann vermutet werden, aber ich glaube es braucht mehr als nur einen Pullover.
341 A: Ja klar, das war jetzt nur ein Beispiel. Hast du schon einmal davon gehört?
342 I: Nein.
343 A: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft deine Freundesliste auf Facebook
344 kontrollieren und auch die Bewegungsdaten von deinem Smartphone heranziehen, wenn sie
345 prüfen wollen, ob du kreditwürdig bist oder nicht?
346 I: Ja.
347 A: Wieso?
348 I: Wenn du vielleicht viele Freunde hast, die nicht kreditwürdig sind, dass vielleicht du auch
349 in die gleichen Verhältnisse oder gleich eingestuft werden kannst. Das muss nicht so sein,
350 aber das ist halt eine Wahrscheinlichkeit.
351 A: Hast du schon einmal davon gehört?
352 I: Nein.
353 A: Du hast gesagt, du hast auch so Gesundheits- und Fitness-Apps. Kannst du dir vorstellen,
354 dass in Zukunft sich Gesundheitsversicherungen mit solchen Apps zusammenschließen, wenn
355 sie prüfen wollen, ob jemand regelmäßig Sport macht und sich gesund ernährt, um zu
356 entscheiden, welche Gesundheitsversicherung jemand bekommt oder ob derjenige überhaupt
357 eine bekommt?
358 I: Kann ich mir auch vorstellen, wenn er ganz miserabel in Form ist zum Beispiel.
359 A: Was nutzt das der Versicherung, wenn sie sich zusammenschließt?
360 I: Risiko ausrechnen, dass sie das vielleicht ein bisschen besser können.
361 A: Hast du schon einmal davon gehört?
362 I: Nein, nie überlegt.
363 A: Dann: Wie wahrscheinlich hältst du das Szenario, dass man in Zukunft in ein Land nicht
364 mehr einreisen darf, weil man zum Beispiel im Internet ein bestimmtes Wort eingegeben hat
365 oder in einer SMS etwas geschrieben hat, zum Beispiel nehmen wir mal an: Ich zerstöre mich
366 in Amerika. Wäre das für dich denkbar?
367 I: Ja!
368 A: Wieso?
369 I: Weil das ein Sicherheitsrisiko darstellt.
370 A: Wie funktioniert das dann?

371 I: Ja auch mit NSA wahrscheinlich, dass sie den Facebook-Chat überprüfen, und dass sie
372 sehen, wenn du in das Flugzeug einsteigst, sie dich dann gleich fassen, wenn du aussteigst
373 oder dass sie dich gar nicht einsteigen lassen.

374 A: Hast du schon einmal davon gehört?

375 I: Nein.

376 A: Gut, dann die letzte Frage: Ist es für dich realistisch, dass man aus dem Verhalten der
377 Vergangenheit, das Verhalten in der Zukunft schon vorhersagen kann, mit einer hoher
378 Wahrscheinlichkeit?

379 I: Möglich, aber nicht sicher, weil Menschen ändern sich auch. Man kann sich halt wieder
380 eine Wahrscheinlichkeit ausrechnen.

381 A: Gut. Danke für das Interview.

1 **Interview 10, am 01.11.2014. Dauer 34:56 Minuten**
2
3 A: Wie alt bist du, und was machst du beruflich?
4 I: Ich bin 20 und studiere in Ort 5 Studium 1.
5 A: Mit welchen Medien informierst du dich vorwiegend?
6 I: Mich selbst?
7 A: Ja.
8 I: Internet, also, wenn ich selbst etwas suchen muss, Internet. Und Fernsehen, aber das ist
9 passiv – Nachrichten. Am meisten Internet.
10 A: Was nutzt du im Internet vor allem?
11 I: Ich benutze das Internet für alles. Vor allem für die Informationssammlung, zur
12 Unterhaltung, ja.
13 A: Mit anderen zu kommunizieren auch?
14 I: Ah, ja richtig. Natürlich zur Kommunikation auch. WhatsApp.
15 A: Hast du zum Beispiel auch so Zeitungen, die du liest, oder Magazine?
16 I: Ich habe, ja habe ich auch, also Zeitungen bei uns die Zeitung 1 und Zeitung 2 habe ich.
17 A: In Ort 5 hast du da auch eine Zeitung, die du liest?
18 I: Nein, habe ich nicht, außer ich finde gerade mal eine, dann lese ich sie.
19 A: Wie oft informierst du dich? Jeden Tag oder ein paar Mal die Woche?
20 I: Wenn wir jetzt die Zeitung hier haben, dann lese ich sie jeden Tag, sonst informiere ich
21 mich unregelmäßig, wie es gerade braucht.
22 A: Du bist ja auch auf Facebook, richtig?
23 I: Ja.
24 A: Hast du auf Facebook zum Beispiel auch Stol oder so eine Nachrichtenseite, die immer
25 wieder mal Nachrichten posten?
26 I: Da habe ich gar ein paar. Ich habe, ja Stol habe ich und weiß jetzt nicht, Corriere della Sera,
27 Alto Adige und weitere.
28 A: Sonst noch was, was dir einfällt? Die Welt zum Beispiel?
29 I: Die Welt, wenn ich mich informiere, komme ich oft auf Die Welt. Die Zeit manchmal.
30 A: Hast du das alles auf Facebook, oder suchst du dir da wirklich die Onlineausgaben der
31 Zeitungen?
32 I: Diese benutze ich nur, also wenn ich irgendetwas suche, das mich gerade interessiert, dann
33 klicke ich auf die Links. Die Welt

34 A: Dann gibst du das praktisch in Google als Suchbegriff ein und gehst dann bei den
35 Ergebnissen auf die Links.

36 I: Ja, genau. Da komme ich ziemlich oft zur Die Welt und Die Zeit. Diese lese ich recht gerne.

37 A: Welches Smartphone besitzt du?

38 I: Marke 1 Model 2

39 A: Für was gebrauchst du dein Smartphone?

40 I: Vorwiegend Kommunikation und im Internet zu surfen. Also Facebook viel und Dinge suchen,
41 YouTube auch. Und zum Spielen benutze ich es auch.

42 A: Zum Spielen, ja. Wecker?

43 I: Wecker, nein.

44 A: Kalender?

45 I: Kalender benutze ich eigentlich weniger.

46 A: Hast du auch Apps heruntergeladen auf dein Smartphone?

47 I: Ja.

48 A: Welche?

49 I: Also, die ich am meisten benutze ist die Facebook App und Facebook Messenger App.
50 WhatsApp, das ich am meisten benutzen werde und dann muss ich suchen. Ja Shazam, finde
51 ich sehr praktisch für die Musik, dann sind diverse Spiele und SoundCloud, Antiviren,
52 Übersetzer, Skype, Spotify.

53 A: YouTube?

54 I: YouTube ist standardmäßig drauf.

55 A: Taschenlampe?

56 I: Ja, Taschenlampe habe ich auch.

57 A: Geburtstagskalender und eine Wetter App hast du das auch?

58 I: Nein, da benutze ich Facebook dazu und Wetter App habe ich automatisch drauf, da habe
59 ich so ein Widget.

60 A: Ok, aber das ist im Grunde auch eine App.

61 I: Ja, das ist auch eine App. Aber wenn ich das Wetter suche, dann gebe ich das bei Google
62 ein.

63 A: Also am meisten brauchst du Facebook, Facebook Messenger, WhatsApp und?

64 I: Normal das Internet.

65 A: Spiele, wie oft nutzt du diese?

66 I: Unregelmäßig.

67 A: Ok, ein paar Mal die Woche?

68 I: Jetzt in letzter Zeit habe ich diese überhaupt nicht genutzt, aber seit ich wieder studiere,
69 mehr.

70 A: Hast du den Begriff Big Data schon mal gehört?

71 I: Big Data habe ich wirklich schon mal gehört, aber ich weiß jetzt nicht genau, mit was ich es
72 in Zusammenhang bringen soll.

73 A: Kannst du dir dennoch vorstellen, was man darunter verstehen könnte?

74 I: Bei Big Data? Ja massive Datensammlung. Meine Meinung.

75 A: Ok. Datenschutz ist dir ein Begriff?

76 I: Ja, Datenschutz ist mir ein Begriff.

77 A: Wie gut kennst du dich mit Datenschutz aus?

78 I: Ich kenne mich mit Datenschutz nicht so gut aus, wenn ich ehrlich bin. Ich vertraue aber
79 auch diesen vielen Unternehmen nicht.

80 A: Erzähl mal: Wenn du jemandem beschreiben müsstest, was Datenschutz ist, was würdest
81 du dann sagen?

82 I: Wenn ich jemandem Datenschutz... Das ist ein von mir und von meinem Vertragspartner,
83 kann man sagen... vor allem Dienste, denen ich meine Daten geben muss, Krankenhaus,
84 Bilder oder so, die Schule, dass die Schule diese nur für den Zweck benutzen, für den ich sie
85 frei gebe und sie meine Daten nicht an Dritte weitergeben. In erster Linie meine Daten nicht
86 an Dritte weitergeben.

87 A: Ok. Und wenn, dann auch nur für diesen Zweck, den du einwilligst.

88 I: Für den ich richtig eingewilligt habe, ja.

89 A: Wie willigst du ein, dass sie deine Daten verwenden dürfen?

90 I: Ja, per ankreuzen und der Unterschrift normalerweise.

91 A: Bei der Datenschutzrichtlinie?

92 I: Ja, wenn du so einen Zettel bekommst, oder im Internet ist das oft auch nur ein Häkchen,
93 das du machen musst, um es zu akzeptieren.

94 A: Was steht in einer solchen Datenschutzrichtlinie drinnen?

95 I: Hm, im Datenschutz steht eben meistens drinnen, dass sie deine Daten nicht an Dritte
96 weitergeben bzw. dass sie diese nicht duplizieren, außer die vom Vertrag festgelegten
97 Rahmenbedingungen.

98 A: Hast du bereits einmal eine Datenschutzrichtlinie unterschrieben?

99 I: Ja, die muss man permanent akzeptieren, das letzte Mal bei Situation 1.

100 A: Und wenn wir nun an deine Apps denken. Hast du dir bereits einmal eine
101 Datenschutzrichtlinie oder eine Nutzungsbestimmung vollständig durchgelesen?

102 I: Nein.

103 A: Welche Datenschutzrichtlinien meinst du, haben deine Apps?

104 I: Ich weiß, dass meine Apps meine Daten an Dritte weitergeben, das ist sicher. Weil erst

105 jetzt, zum Beispiel bei Google, wenn man sich bei Google ein Konto macht, bekommt man ja

106 auch diese Sachen, weil in Ort 5 habe ich Objekt 1 gesucht und dann habe ich bei allen

107 Webseiten genau dieses Objekt 1 gesehen, und es war permanent Werbung, dass ich das

108 kaufen soll. Also glaube ich sehr wohl, dass diese das an Dritte weitergeben, halt an

109 Unternehmen, an größere.

110 A: Wo kann man sich über diese Datenschutzrichtlinie jetzt z.B. von Apps informieren?

111 I: Bei der Verbraucherschutzzentrale oder bei den Nutzungsbedingungen, wenn man sie sich

112 durchlesen würde.

113 A: Also auch bei der App selbst, dann?

114 I: Ja, müsste möglich sein.

115 A: Auf welche Daten haben dann deine Apps Zugriff? Auf was können sie zugreifen?

116 I: Da wird ja jetzt bei Google immer ein Fenster geöffnet, in dem steht worauf sie zugreifen

117 können. Auf Mitteilungen können viele schon zugreifen, es können auch viele auf den

118 Suchverlauf vom Internet zugreifen und auch ein paar auf Kreditkarten, also, wenn man im

119 Internet bezahlt, auf das können auch einige zugreifen. Ja, und Medien auch.

120 A: Ja, vom Smartphone direkt?

121 I: Ja.

122 A: Was fällt bei dir unter Medien alles rein?

123 I: Was ich auf dem Handy habe. Medien. Also ich habe weder Videos noch Musik auf dem

124 Handy, weil das habe ich alles auf dem Gerät 1.

125 A: Aber auf Fotos schon dann?

126 I: Ja, glaube ich schon.

127 A: Ok. Du hast gesagt, du nutzt dein Smartphone auch Fotos zu machen.

128 I: Ja, weniger.

129 A: Aber ein paar machst du schon, oder?

130 I: Ja.

131 A: Angenommen, der Max nutzt sein Handy immer nur zu Hause und alleine, ohne, dass sich

132 jemand anderer neben ihm oder im gleichen Raum aufhält. Denkst du, ist es dann dennoch

133 möglich, dass andere seine Fotos sehen können, ohne dass er es ihnen zeigt oder schickt?

134 I: Andere Personen. Privatpersonen oder Unternehmen?

135 A: Unternehmen, zum Beispiel.

136 I: Wenn er das mit Internet benutzt, über Internet, und er sich... Ich weiß jetzt nicht. Kannst
137 du mir die Frage ein bisschen genauer stellen?

138 A: Wenn er jetzt zum Beispiel auf seinem Handy auch Apps und so heruntergeladen hat und
139 Fotos macht, meinst du, ist es dann möglich, dass andere Leute seine Fotos sehen, obwohl er
140 ihnen diese nie schickt oder zeigt?

141 I: Möglich ist es sicher.

142 A: Kannst du dir auch vorstellen wie?

143 I: Durch. Erstens durch das Raufladen der App. Die App haben halt Dings, wenn die App,
144 wenn du der App erlaubst, auf das zuzugreifen und die können dann auf die App zugreifen,
145 dann werden sie sich sicher, unter Anführungszeichen, sich in ein Handy rein hacken können,
146 wenn sie wollen würden.

147 A: Kannst du dir vorstellen, dass das auch alles erlaubt ist, was sie machen? Also, dass sie das
148 nicht hacken, und etwas Unerlaubtes tun, sondern, dass der Max ihnen das sogar erlaubt, seine
149 Fotos anzusehen, aber ihm ist es nicht wirklich bewusst?

150 I: Dass er ihnen das erlaubt, ihm das aber nicht bewusst ist, darin bin ich voll überzeugt, dass
151 das der Fall ist. Ob das rein verfassungstechnisch erlaubt ist, was die machen, ist fragwürdig.

152 A: Wie meinst du, ist das möglich, dass er es ihnen erlaubt, aber es ihm gar nicht bewusst ist?

153 I: Durch die allgemeine Nutzerbedingung, durch die AGB.

154 A: Dass er sich das nie durchliest, dass er es dann nicht weiß?

155 I: Genau.

156 A: Wie gut meinst du, sind deine Fotos auf deinem Smartphone vor der Einsichtnahme
157 anderer Personen geschützt?

158 I: Meine? Nicht unbedingt gut, aber ich habe auch nichts zu verbergen, eigentlich.

159 A: Wer bestimmt die Sicherheit deiner Fotos und anderer Daten auf deinem Smartphone?

160 I: Ja eigentlich ich selbst, wie viel ich rauflade an Apps, was diese Apps machen und ich
161 könnte sie sicher ja auch theoretisch irgendwie verschlüsseln oder den Zugriff verweigern,
162 quasi, wenn man sich ein bisschen informieren würde.

163 A: Ja, genau, weil hast du dann eine Möglichkeit diese zu kontrollieren?

164 I: Es gibt, einige von diesen AntiVierenApp sagen dir, welche von diesen Programmen auf
165 was zugreifen können.

166 A: Und dann siehst du auch was die herunterladen oder von wo wie viel Speicher sie sich
167 herunterladen?

168 I: Nein, das sieht man nicht, was sie runterladen von deinem Handy, nur auf was sie
169 theoretisch zugreifen können.

170 A: Ok, kannst du von deinem Handy auch sehen, zum Beispiel diese App ladet sich so und so
171 viel Megabyte herunter.

172 I: Nein, das ist glaube ich nicht möglich. Nein, weiß ich nicht genau.

173 A: Wieso meinst du, brauchen Apps Zugriff auf verschiedene Bereiche?

174 I: Ja wegen der Wirtschaft in erster Linie. Ich meine solche Unternehmen wie Facebook oder
175 so, diese müssen sich irgendwie finanzieren, eigentlich das ist ja gratis das ganze Ding, sie
176 brauchen aber doch für diese ganze Serverkapazität, brauchen sie Geld. Dein Account und
177 das. Das machen sie einmal durch aktive Werbeschaltung und durch die Information, durch
178 deine Verbrauch-Information, an Unternehmen und dann bekommst du ja diese
179 maßgeschneiderte Werbung zu dir geliefert, dass sie dich mehr oder weniger genau mit dem
180 bombardieren, für was du dich informierst, jetzt eine Hausfrau werden sie nicht, keine
181 Ahnung, mit Werbung von Dings einschalten wollen, für was weiß ich, Auto, Sportauto.

182 A: Ok. Das heißt, wenn eine Taschenlampen App sagt, sie braucht Zugriff auf das Internet,
183 kannst du das dann nachvollziehen, dass sie das braucht, weil sie funktionieren muss?

184 I: Nein, für eine Taschenlampen App nicht.

185 A: Wieso meinst du dann, braucht sie Zugriff auf das Internet?

186 I: Ja genau wegen so was. Weil eine Taschenlampen App braucht überhaupt keinen Zugriff
187 auf das Internet, das macht Null Sinn, wenn ich ehrlich bin.

188 A: Du hast gesagt diese Apps nutzen deine Daten für Werbung.

189 I: Ja.

190 A: Kannst du dir ein anderes Ziel, außer Werbung, noch vorstellen? Dass es da noch ein
191 anderes Ziel gibt, dass es praktisch nicht nur die Werbung gibt, die interessant ist für sie?

192 I: Naja, für den Staat, wie man jetzt bei den NSA herausgefunden hat, ist Spionage auch
193 interessant. Wie man da gehört hat, haben sie da auch auf die Google-Server zugegriffen.

194 A: Was wollen sie im Grunde mit Spionage erreichen?

195 I: Ja, das eine ist Wirtschaftsspionage, nicht direkt aber halt so. Und das andere ist die aktive
196 Kontrolle von der Masse. Wenn du die Masse kontrollieren kannst, beziehungsweise ihre
197 Gedanken nachvollziehen, hast du als Staat mehr Macht und mehr Kontrolle über dein
198 eigenes Volk.

199 A: Was meinst du, können Unternehmen machen, wenn sie unzählig viele Daten von unzählig
200 vielen Leuten besitzen? Was meinst du machen diese mit denen?

201 I: Ja zuerst mal in Datenbanken einspeichern, Datenbanken vergleichen und durch
202 irgendwelche komplizierte Programme durchlaufen lassen, die Programme dann noch
203 filtern, was du so suchst. Und dir dann automatisch wieder – ihnen Information mehr oder

204 weniger was diese Person, natürlich macht das alles ein Computer, weil für einen Menschen
205 wäre das zu viel.

206 A: Das heißt die werden gut verarbeitet und analysiert?

207 I: Ja, sie werden analysiert und verarbeitet, ich meine natürlich wird von Person XY, werden
208 jetzt nicht Mitarbeiter, Bilder zu sehen bekommen. Sie können es, wenn sie wollen, aber ich
209 glaube nicht, dass mein Bild irgendjemand, keine Ahnung, der in Kalifornien in einer Zentrale
210 arbeitet, alle meine Bilder sieht. Natürlich können sie es, wenn sie wollen, aber ich sage, das
211 wird automatisch verarbeitet.

212 A: Hast du dir schon mal überlegt, einen Dienst oder eine App deswegen aufzugeben oder zu
213 löschen?

214 I: Ja, wenn ich über das Dings, über das Antivirenprogramm wirklich Dings bekomme,
215 wirklich aktiv, das Dings, diese App, hat unnütze Zugriffe und mir die App nicht unbedingt
216 mega einleuchtet, dann lösche ich sie.

217 A: Ok, hast du dieses Virenprogramm extra wegen dem installiert, damit du da eine Übersicht
218 hast?

219 I: Nein, das Virenprogramm, ich habe das Virenprogramm installiert, damit ich ein
220 Virenprogramm habe.

221 A: Was müsste passieren, dass du sagst, ok Facebook, das ging jetzt eindeutig zu weit, das
222 lasse ich jetzt. Oder WhatsApp, eines von diesen beiden.

223 I: Hmm. Was muss da unbedingt passieren? Es muss passieren, wenn ich wirklich etwas zu
224 verbergen hätte, was ich jetzt nicht habe, werde ich es sicher nicht benutzen. Zum Beispiel,
225 wenn ich jetzt, keine Ahnung, einen Terroranschlag planen will, dann werde ich das sicher
226 nicht über WhatsApp ausmachen.

227 A: Dass, also praktisch deine Persönlichkeit geschützt wird, das ist wichtig.

228 I: Ja.

229 A: Und nehmen wir mal an, du hast Fotos auf deinem Smartphone, die zwar nicht schlimm
230 sind, du aber dennoch nicht möchtest, dass diese in die Öffentlichkeit gelangen, wenn du
231 diese Fotos aber auf einmal öffentlich sehen würdest, oder du weißt, dass diese Fotos andere
232 Personen gesehen haben, weil sie Zugriff auf dein Smartphone hatten, wäre das für dich so
233 ein Grund, dass du sagst, ok, das geht jetzt zu weit, ich möchte mich mehr schützen.

234 I: Auf jeden Fall.

235 A: Hast du dir sonst noch, außer der Viren App was überlegt, wie du dich in Zukunft vor
236 dieser Datenspeicherung schützen möchtest?

237 I: Ja, es ist. Nein überlegt habe ich nicht, aber ich würde es schon tun, wenn ich etwas finden
238 würde, würde ich das schon tun, was einfach ist und nicht zu kompliziert ist.

239 A: Aber im Grunde die Datenschutzrichtlinien von den Apps, würdest du diese zum Beispiel
240 in Zukunft durchlesen, damit du Bescheid weißt, oder bist du immer noch der Meinung, dass
241 auf deinem Handy einfach nicht so viel drauf ist, was sie nehmen könnten und es dich stören
242 würde.

243 I: Ich lese mir die Datenschutzrichtlinien sicher nicht durch.

244 A: Wie denkst du wird unser Leben mit dem Smartphone in 30, 50 Jahren aussehen?

245 I: Da wird es gar keine Smartphones mehr geben. Vielleicht nur mehr Chips, die in uns
246 eingebaut sind, oder Brillen gibt es ja heute schon. Da werden sie uns noch viel mehr und
247 stärker überwachen als sie es heute schon tun.

248 A: Ok, ich schildere dir nun ein paar Szenarien und frage dich, ob du diese für möglich hältst
249 oder nicht.

250 Wenn jemand täglich das Smartphone mit Apps und Internet zum Beispiel Twitter und/oder
251 Facebook nutzt, ohne jedoch jemals seinen Standort preiszugeben. Wäre es für dich dann
252 doch vorstellbar, dass man mit großer Wahrscheinlichkeit vorhersagen kann, wo sich
253 derjenige in Zukunft aufhalten wird?

254 I: Ja.

255 A: Wieso?

256 I: Ein Handy rückverfolgen geht immer, also auch mit Dings, und nur weil du aktiv nicht
257 deinen Standort preisgibst, heißt das nicht, dass es a) keine Lücke in der
258 Datenschutzbestimmung gibt und b) wenn man will, kann man dennoch deinen Standort
259 herausfinden.

260 A: Könntest du dir zum Beispiel vorstellen, dass man schon nur, also wenn man zum Beispiel
261 selbst sein eigenes Handy verloren hat, man kann also keine Daten oder den Standort mehr
262 preisgeben, kannst du dir vorstellen, dass man schon allein durch die Informationen von ein
263 paar engen Facebook-Freunden herausfinden kann, wo sich derjenige wahrscheinlich in
264 Zukunft aufhalten wird.

265 I: In Zukunft aufhalten wird?

266 A: Ja, genau. Also nicht im Moment, sondern zum Beispiel morgen. Dass man sagen kann die
267 Wahrscheinlichkeit, dass diese Person morgen an diesem Standort ist, ist 50 oder 80 Prozent
268 groß.

269 I: Also von engen Freunden, kann sein, finde ich jetzt aber nicht so wahrscheinlich, solange
270 sie dir keine Nachrichten schicken, ob du morgen da oder dort hinkommst.

271 A: Ja, also nur zum Beispiel durch den Standort der Facebook-Freunde kann man das nicht
 272 sagen, mit einer gewissen Wahrscheinlichkeit ist diese Person morgen dort?

273 I: Ah durch die Dings? Ja, aber wenn ich natürlich in letzter Zeit enge Freunde in Australien
 274 oder so hinzugefügt habe, dann werde ich mich höchstwahrscheinlich gerade in Australien
 275 aufhalten. Aber ich sage jetzt so, dass sie mir sagen können, wo ich morgen bin, nur durch ein
 276 paar enge Facebook-Freunde und ich mein Handy im nirgendwo lasse, finde ich nicht so
 277 wahrscheinlich.

278 A: Hast du schon einmal davon gehört?

279 I: Was?

280 A: Dass man das vorhersagen kann?

281 I: Nein, dass man es nachvollziehen kann, dass man genau eine Map erstellen kann, wo er
 282 war, das schon, aber dass man Vorhersagen machen kann, das habe ich noch nie gehört.

283 A: Wie realistisch ist es für dich, dass die Polizei bereits heute schon wissen kann, wo morgen
 284 ein Verbrechen stattfindet? Da sprechen wir aber jetzt nicht unbedingt von Ort 6, sondern von
 285 vielleicht wirklich von L.A., Kalifornien, USA, sowas.

286 I: So wie beim Minority Report? Es kann theoretisch schon möglich sein durch aktive
 287 Kontrolle von fragwürdigen Personen, weil, und durch Datensammlung von diesen Personen,
 288 kann es theoretisch schon, können sie eine größere Wahrscheinlichkeit haben, dass derjenige
 289 in nächster Zeit ein Verbrechen begeht, als nicht. Dass sie genau sagen können, morgen findet
 290 ein Verbrechen statt, da muss er schon sehr bescheuert sein. Da muss er schon allen seinen
 291 Kollegen schreiben, ich gehe morgen die Bank ausrauben.

292 A: Wäre es für dich vorstellbar, dass, wenn die Polizei beginnt die letzten Jahre zu
 293 untersuchen und zu schauen wo in der Stadt, nehmen wir mal Miami her, wo dort die
 294 Verbrechen stattfanden und zeichnen das alles auf und nehmen diese Daten her und schauen
 295 ob es eine Möglichkeit gibt herauszufinden, wo in Zukunft die Verbrechen stattfinden
 296 könnten. Das ist dann nicht so, dass sie 100 prozentig an jener Kreuzung stattfinden, aber mit
 297 einer Wahrscheinlichkeit von 80 Prozent findet in diesem Raum ein Verbrechen statt.

298 I: Auf jeden Fall, ja.

299 A: Wie funktioniert das?

300 I: Ja, du tust da Dings, sagen wir, du nimmst von den letzten 20 Jahren alle
 301 Verbrechensstandorte und analysierst diese und trägst sie mit roten Punkten auf einer Karte
 302 ein, dann wirst du irgendwann, rein statistisch, wirst du irgendwann eine Zone bekommen, wo
 303 du mehr Verbrechen hast. Das ist dann deine rote Zone. Zum Beispiel als Zone, kannst du
 304 sagen in Amerika in irgendwelchen Armenvierteln, wie Bronx früher oder etwas. Natürlich

305 sind da dann mehr Verbrechen, das ist dann so. Oder in einer Zone, die eher abgeschieden ist,
306 aber dennoch viele wertvolle Sachen sind oder so. Und wenn du dann halt jedes Verbrechen
307 analysierst, einträgst, dann wirst du schon statistisch irgendwo Ballungsräume für
308 Kriminalität haben.

309 A: Hast du davon schon mal gehört?

310 I: Das vom Dings, glaube ich, habe ich wirklich schon einmal gehört, dass die Polizei eben
311 sowas, ja genau! In L.A., jetzt weil du es sagst, dass die Polizei alle Daten sammelt und diese
312 Gebiete wirklich stärker kontrollieret, während andere schwächer kontrolliert werden.

313 A: Gut, dann das dritte Beispiel: Nehmen wir an eine Frau kauft im Supermarkt verschiedene
314 Sachen ein, jedoch keinerlei Babysachen. Kannst du dir vorstellen, dass man nur aus den
315 gekauften Artikeln mit hoher Wahrscheinlichkeit sagen kann, ob diese Frau schwanger ist und
316 ungefähr ob sie sich in der frühen Schwangerschaft, in der Mitte oder eher am Ende der
317 Schwangerschaft befindet?

318 I: Da müsste man wissen, ob auf der... natürlich müsstest du per Kreditkarte zahlen, oder mit
319 Dings. Es hängt vom Laden ab. Wenn du das im Supermarkt einkaufst und es werden genau
320 alle, es werden ja alle Nahrungsmittel eingescannt, und wenn du dann noch ein Foto hast, von
321 dieser Person, von einer Überwachungskamera und du ihre Nahrungsmittel siehst, dann wirst
322 du das schon vorhersagen können. Das wird aber nur in großen Nahrungsmittelgeschäften
323 gehen, Supermärkte, es wird aber nicht gehen, wenn ich beim kleinen Geschäft im Dorf
324 einkaufe.

325 A: Ist es auch möglich, wenn diese Frau im Supermarkt bar bezahlt und ihr Gesicht nicht
326 erkannt wird? Kannst du dir das dann dennoch vorstellen?

327 I: Nein, kann ich mir nicht vorstellen.

328 A: Wieso nicht?

329 I: Weil man braucht. Wenn sie dann auch noch kein Handy hat, das sie gerade mitführt, also
330 ohne Technik den Supermarkt betritt, dann kann ich mir das nicht vorstellen, weil sie braucht
331 ja, man braucht irgendwie eine Bezugsperson, zu der, die das gekauft hat. Und wenn keine
332 Kameras vorhanden sind und auch kein Handy, das den Standort verraten könnte, im
333 schlimmsten Fall, dann kann ich mir das nicht vorstellen.

334 A: Hast du schon einmal davon gehört?

335 I: Von dem mit dem Essen und dass eine Frau schwanger ist, nein, hab ich noch nie gehört.

336 A: Ok, dann gehen wir zum nächsten Beispiel: Nehmen wir an, ein Mann ist homosexuell, er
337 nützt das Internet, darunter auch Social Media, aber gibt jedoch nirgends an, dass er Männer
338 liebt. Sein Sexualleben wird von ihm nicht preisgegeben, er hält das sehr geheim, gibt also

339 weder im Internet, noch sonst irgendwo etwas an. Für wie realistisch hältst du es, dass
340 wildfremde Personen dennoch mit hoher Wahrscheinlichkeit sagen können, dass der Mann
341 homosexuell ist?

342 I: Solange er im Internet nicht auf, nicht auf, ich meine Seiten, wie, irgendwelche
343 Homosexuellenforen zwar anonym geht, also sich nicht dort anmeldet. Oder andere Seiten,
344 die dies zum Thema haben, oder auf Facebook unbedingt Fotos von Männermodels sucht, er
345 muss sie ja nicht liken, dann ist das schon wahrscheinlich, wenn er das alles nicht macht, ist
346 das relativ unwahrscheinlich.

347 A: Könntest du dir vorstellen, dass es da auch eine andere Möglichkeit gibt? Zum Beispiel,
348 wenn man 10.000 homosexuelle Männer untersucht und man findet heraus, dass sie gerne,
349 jetzt nur als Beispiel, mehr Körperpflegeprodukte kaufen als der durchschnittliche Mann,
350 gerne tanzen gehen und einen sehr modischen Geschmack beim Outfit haben. Und wenn man
351 jetzt einen Mann überprüft, gibt er zwar nicht an, dass er homosexuell ist, stimmt aber in allen
352 drei Kategorien überein. Wäre es für dich dann denkbar, dass man mit einer gewissen
353 Wahrscheinlichkeit sagen kann, dass der Mann homosexuell ist?

354 I: Weil er viele Körperpflegeprodukte kauft? Nein.

355 A: Wieso nicht?

356 I: Ich wüsste nicht welche Verbindung diese Sachen mit Homosexualität zu tun haben. Ich
357 meine alle diese Sachen können auch andere Männer gerne tun, deswegen müssen nicht alle
358 homosexuell sein.

359 A: Hast du schon einmal davon gehört?

360 I: Nein.

361 A: Kannst du dir vorstellen, dass ein Kreditinstitut in Zukunft deine Freundesliste auf
362 Facebook kontrollieren und auch die Bewegungsdaten von deinem Smartphone heranziehen,
363 wenn sie prüfen wollen, ob du kreditwürdig bist oder nicht und ob du überhaupt einen Kredit
364 bekommst?

365 I: Bei Banken kann ich mir das gut vorstellen.

366 A: Wieso?

367 I: Besonders bei großen Banken, weil große Banken doch eigentlich viel Macht besitzen, es
368 ist eigentlich nur die Wirtschaft, die die Welt da kontrolliert, meiner Meinung nach und auch
369 die Politik von der Wirtschaft aus geht und Banken haben da eine zentrale Rolle und können
370 diese Macht ausnutzen, um eben der passenden Person das zu geben und das werden sie auch
371 machen, solange die Kosten von der Kontrolle der Person nicht die möglichen Schäden
372 übersteigen. Natürlich, wenn ich eine Million Euro brauche, um jemanden zu kontrollieren,

373 derjenige mir aber nur maximal einen Schaden von 100.000 Euro machen kann, dann hat das
374 keinen Sinn.

375 A: Ja, weil das Verhältnis zwischen Kosten und Nutzen nicht passt. Aber zur Sicherheit von
376 ihnen, kannst du dir das vorstellen?

377 I: Ja, bei der Bank kann ich mir das gut vorstellen.

378 A: Hast du schon einmal davon gehört?

379 I: Nein, habe ich nicht.

380 A: Kennst du die Gesundheits- und Fitness-Apps, die man am sich auf das Smartphone
381 herunterladen kann?

382 I: Ja, ich habe sogar mal eine runtergeladen.

383 A: Kannst du dir vorstellen, dass sich in Zukunft Gesundheitsversicherungen mit solchen
384 Arten von Apps zusammenschließen, wenn sie prüfen wollen, ob jemand regelmäßig Sport
385 macht und ob derjenige sich gesund ernährt, wenn sie schauen wollen, welche Versicherung
386 diese Person bekommt, oder ob sie überhaupt eine bekommt?

387 I: Das kann sein, macht für mich aber nicht so viel Sinn, nur weil ich eine solche Fitness-App
388 drauf habe, glaube ich machen das die wenigsten. Finde ich nicht so wahrscheinlich.

389 A: Aber du kannst dir das vorstellen, dass die Gesundheitsversicherungen damit beginnen?

390 I: Vorstellen kann ich mir das schon. Aber es ergibt in meinen Augen nicht so viel Sinn.

391 A: Wieso nicht?

392 I: Weil momentan viele Leute auch ins Fitnessstudio gehen und durch so eine App weiß ich
393 halt doch nichts. Am Anfang vielleicht benutzen sie es, aber sobald sie das Zirkeltraining
394 auswendig können, dann werden sie das ohne die App machen.

395 A: Hast du schon einmal davon gehört?

396 I: Hab ich auch noch nie gehört.

397 A: Wie wahrscheinlich hältst du das Szenario, dass man in Zukunft in ein Land, wie zum
398 Beispiel in die USA, nicht mehr einreisen darf, weil man zum Beispiel ein bestimmtes Wort
399 im Internet eingegeben hat oder per SMS geschrieben hat?

400 I: Nur ein bestimmtes Wort?

401 A: Ja, ein Wort oder einen Satz.

402 I: Ich weiß, dass die Amerikaner relativ viel kontrollieren, auch schon solche Sachen, schauen
403 auch schon deine Tattoos an, wenn du am Flughafen bist, hab ich mal gehört und deshalb finde
404 ich das in Kontrollstaaten, wie Amerika, Nordkorea, China, vielleicht bei denen finde ich das
405 nicht so unwahrscheinlich.

406 A: Wenn wir zwei jetzt zum Beispiel gerne nach Amerika fahren würden und ich schreibe dir
407 eine SMS vorher noch, und sage darin: Wir werden uns in Amerika voll zerstören, meine
408 damit aber, dass wir feiern gehen werden und uns in dem Sinn mit dem Alkohol zerstören
409 werden, meinst du, könnte das für uns problematisch werden, dass wir nicht mehr einreisen
410 dürfen, zum Beispiel?

411 I: Das ist jetzt eine schwierige Frage, hängt davon ab, wie blöd diese Leute sind, bei diesem
412 Unternehmen. Es kann problematisch werden, aber ich glaube jetzt in den nächsten fünf
413 Jahren nicht.

414 A: Wieso nicht?

415 I: Weil ich mir denke, dass es ein zu schlechtes Bild machen würde, erst jetzt nach dem NSA-
416 Skandal, wenn sie unschuldige Personen nicht einreisen lassen, besonders, wenn sie aus
417 europäischen Staaten kommen. Es macht auch sicher einen Unterschied, wenn sie vom nahen
418 Osten sind. Aber ich glaube es macht ein extrem schlechtes Bild erst jetzt nach diesem
419 Skandal, wenn sie irgendwelche Leute nicht einreisen lassen, durch irgendwelche komischen
420 Gründe, für die sie keine Beweise haben, dir aber auch keinen logischen Grund liefern
421 können, sondern einfach nur sagen, du darfst nicht einreisen.

422 A: Aber wenn ich schreibe: Ich werde mich in Amerika zerstören, dann hätten sie wohl einen
423 Grund. Dann könnten sie ja sagen Terrorangriff.

424 I: Wir werden Amerika zerstören, nur diesen Satz finde ich als Grund relativ bei den Haaren
425 herangezogen.

426 A: Gut, dann das letzte Beispiel: Ist es für dich realistisch, dass man aus dem Verhalten der
427 Vergangenheit, schon das Verhalten in der Zukunft vorhersagen kann mit einer gewissen
428 Wahrscheinlichkeit immer?

429 I: Ja.

430 A: Wieso?

431 I: Wenn ich jetzt seit 10 Jahren immer am Mittwoch schwimmen gehe, dann werde ich das
432 auch in den nächsten Jahren so tun, wahrscheinlich.

433 A: Hast du davon schon mal gehört?

434 I: Nein, eigentlich nicht wirklich.

435 A: Danke dir für das Interview.

1 **Interview 11, am 09.11.2014. Dauer 33:38 Minuten**

2

3 A: Wie alt bist du, und was machst du beruflich?

4 I: Ich bin 19 und bin Student.

5 A: Was studierst du?

6 I: Studium 2.

7 A: Mit welchen Medien informierst du dich vorwiegend?

8 I: Handy. Also eigentlich nur Internet, und sonst, Nachrichten schau ich eigentlich gar nicht,
9 Zeitungen lese ich auch nicht. Also eigentlich nur Internet, Handy.

10 A: Ok, was schaust du da?

11 I: Stol, bei uns, halt mich zu informieren und sonst eigentlich nichts. Das ist die einzige Seite,
12 Plattform, wo ich mich informiere.

13 A: Bist du bei Facebook?

14 I: Ja.

15 A: Hast du da zum Beispiel auch Zeitungen oder Infoportale geliked, die dann immer wieder
16 mal eine Nachricht posten?

17 I: Stol habe ich geliked, und dann, ja, Wetterdienste, aber sonst eigentlich nichts. Ich glaube,
18 ich like relativ wenig, deshalb sind es nur diese zwei Sachen.

19 A: Machst du das täglich, dass du dich dort informierst?

20 I: Ach, nur wenn mir langweilig ist. Also ich informiere mich nicht, weil es mir wichtig ist,
21 sondern mehr als Zeitvertreib. Wenn ich in der Uni sitze und es ist gerade nicht so interessant,
22 dass ich kurz auf Stol reinschaue und schaue was in Ort 6 los ist. Es ist nicht, so, dass ich
23 mich immer informieren will. Es ist oft wirklich nur der Zeitvertreib.

24 A: Hörst du Radio?

25 I: Gar nicht, ich hör nicht Radio, ich höre nur meine Musik.

26 A: Welches Smartphone besitzt du?

27 I: Marke 3 Model 3.

28 A: Für was gebrauchst du dein Smartphone?

29 I: Also hauptsächlich für, also in dem Sinn, nur für den Zeitvertreib, aber zum Chatten, WhatsApp,
30 Facebook. Das sind eigentlich die wichtigsten, Instagram noch und sonst nichts. Telefonieren ab und
31 zu.

32 A: SMS schreiben?

33 I: Das gar nicht mehr. Nur mehr WhatsApp, Facebook. SMS gar nicht mehr.

34 A: Wecker oder so?

35 I: Natürlich, Wecker.
36 A: Hast du auch Apps auf dein Smartphone heruntergeladen?
37 I: Ja, aber nicht viele, nur die wichtigsten, die ich immer brauche.
38 A: Was hast du dir da runtergeladen?
39 I: Eigentlich nur Facebook, Instagram, WhatsApp, dann Stol natürlich, aber sonst eigentlich
40 vielleicht drei, vier unbewusste Apps, die man nie braucht, und das wars.
41 A: Wetter App oder so was?
42 I: Das war schon eine oben.
43 A: Taschenlampe?
44 I: Ja, von dem ist auch was oben, aber das benütze ich nie.
45 A: Geburtstagskalender dann wahrscheinlich auch nicht?
46 I: Das macht es bei mir alles automatisch bei Facebook. Das ist ganz geschickt. Also Spiele
47 habe ich auch keine oben. Das auch nicht.
48 A: Wie oft verwendest du sie?
49 I: Eigentlich nur, wenn ich gebraucht werde. Also wenn mich jemand anschreibt, dann
50 schreibe ich halt zurück, aber sonst eigentlich nicht, dass ich ständig online bin.
51 A: Aber das ist dann schon jeden Tag, dass dich jemand braucht?
52 I: Ja, das schon, das schon.
53 A: Hast du den Begriff Big Data schon einmal gehört?
54 I: Nein.
55 A: Kannst du dir dennoch etwas darunter vorstellen?
56 I: Viele Daten, ich weiß nicht. Ansammlung von vielen Daten.
57 A: Ok. Datenschutz ist dir ein Begriff?
58 I: Ja.
59 A: Wie gut kennst du dich mit Datenschutz aus?
60 I: Gut, aber ich lege wenig Wert darauf, also mir ist das relativ egal.
61 A: Wenn du jemandem erzählen müsstest, was Datenschutz ist, was würdest du dann sagen?
62 I: Das ist halt ein Bereich, der meine Daten, die ich eingebe, die ich versende, schützen sollte.
63 A: Datenschutzrichtlinie hast du schon mal gehört?
64 I: Das wird halt das Gesetzliche vom Datenschutz sein oder die Vorgaben, wie sagt man? ...
65 A: Was meinst du, steht in einer Datenschutzrichtlinie drinnen?
66 I: Dass meine Daten nicht weitergegeben werden, ich weiß nicht. Ich schau mir das nie an,
67 aber ich denk halt mal, dass meine Daten nicht weitergegeben werden, dass sie gesichert sind.
68 A: Was heißt für dich gesichert?

69 I: Dass niemand darauf zugreifen kann. Auch intern bei den Unternehmen, dass niemand
70 darauf zugreifen darf oder meine Daten benützt, um sie zu verkaufen oder sonst was damit zu
71 machen.

72 A: Kannst du dir vorstellen, dass das vielleicht drinnen steht, wir verwenden deine Daten für
73 xy.

74 I: Könnte ich mir schon vorstellen, dass das drinnen steht. Aber ich glaube, dass das viele
75 Leute nicht lesen, das einfach überspringen, weil es ihnen egal ist.

76 A: Hast du schon mal eine Datenschutzrichtlinie unterzeichnet?

77 I: Ja! Das schon.

78 A: Wo?

79 I: In der Schule hat man das machen müssen, sonst manchmal, wenn man in Ort 9 geht, dass
80 wenn Fotos gemacht werden, dass man da halt etwas unterschreiben muss, aber eigentlich nur
81 das jetzt.

82 A: Du hast gesagt eine Datenschutzrichtlinie hast du dir noch nie vollständig durchgelesen,
83 oder?

84 I: Nein.

85 A: Wenn wir nun an deine Apps denken, was meinst du haben deine Apps welche
86 Datenschutzrichtlinien?

87 I: Relativ schwache wahrscheinlich.

88 A: Das heißt?

89 I: Je nachdem welche Apps, ich meine jetzt sicher bei einigen Apps, Facebook, weiß man halt
90 Bescheid durch die Medien und so, dass es da immer wieder mal Probleme gibt, aber bei den
91 kleineren Apps, ich weiß nicht, wird schon viel weitergegeben. Da ist nicht eine gute
92 Sicherung.

93 A: Praktisch, dass dann andere unbefugt die Daten bekommen?

94 I: Ich denke schon, oder dass sie weitergegeben werden. Oder dass man halt von außen leicht
95 zugreifen kann, dass sie nicht ganz sicher untergebracht sind.

96 A: Wenn sie weitergegeben werden, meinst du dann, dass sie bewusst weitergegeben werden
97 oder nicht?

98 I: Ich denke nicht bewusst, ich denke eher unbewusst. Vielleicht gestohlen, kann auch sein,
99 dass die Sicherung da nicht ganz einwandfrei läuft.

100 A: Wo kann man sich zum Beispiel über die Datenschutzrichtlinie von den Apps
101 informieren?

102 I: Ich denke mal bei der App selbst, dass es vielleicht einen Butten gibt oder so was, dort wo
103 das Formular draufsteht, wo man es sicher irgendwo lesen kann. Ansonsten kann man sich
104 sicher im Internet informieren, jemand kennt sich sicher aus.

105 A: Wenn wir nun an deine Apps denken, steht in den Datenschutzrichtlinien ja drinnen, dass
106 sie Zugriff auf diesen und jenen Bereich brauchen, um funktionieren zu können. Auf welche
107 Daten oder auch welche Bereiche haben jetzt deine Apps Zugriff?

108 I: Fotos. Also wenn ich jetzt Instagram oder so was benütze, dann kommt immer die
109 Meldung, dass sie Zugriff auf die Fotos brauchen und das ist eigentlich bei diesen Apps
110 ständig.

111 A: Musst du das jedes Mal erlauben?

112 I: Nein, man kann es einmal einstellen, dass das so gespeichert wird. Wäre ja anstrengend,
113 wenn man das jedes Mal machen müsste. Aber eigentlich nur Fotos wirklich, wo ich es
114 bewusst mitbekomme, dass sie auf die Fotos zugreifen, aber sonst? Bei den Kontakten glaube
115 ich passiert das nie, dass man darauf zugreift, obwohl WhatsApp greift auf die Kontakte zu,
116 aber sonst eigentlich Fotos hauptsächlich.

117 A: Kannst du dir auch vorstellen, dass sie Zugriff auf die Kamera, Videokamera, Tonband,
118 Internet usw. benötigen?

119 I: Ja, Fotos immer im Bezug auf die Kamera auch.

120 A: Ok, aber auch, die Fotos, die du auf dem Smartphone drauf hast?

121 I: Genau.

122 A: Machst du Fotos mit deinem Smartphone?

123 I: Ja.

124 A: Kannst du dir vorstellen, angenommen, der Max benützt sein Handy immer nur zu Hause
125 und alleine, ohne, dass sich jemand anderer neben ihm oder im gleichen Raum aufhält.
126 Denkst du, ist es dann dennoch möglich, dass andere, wildfremde Personen seine Fotos sehen
127 können, ohne dass er sie ihnen zeigt oder schickt?

128 I: Sicher!

129 A: Wie meinst du funktioniert das?

130 I: Hacken, ich weiß nicht. Es gibt sicher hundert Möglichkeiten. Also hauptsächlich hacken.

131 A: Also illegal dann, oder?

132 I: Illegal natürlich.

133 A: Kannst du dir vorstellen, dass der Max ihnen das sogar erlaubt, die Fotos anzusehen, es
134 ihm aber nicht bewusst ist?

135 I: Wenn er etwas unterschreibt und sich das nicht durchliest, sicher.

136 A: Wie gut meinst du sind deine Fotos auf deinem Smartphone vor der Einsichtnahme anderer
137 geschützt?

138 I: Schlecht. Ich glaube nicht gut, bin ich der Meinung. Ich mach halt auch nichts dafür, glaube
139 ich, ich habe nie was durchgelesen, also, wenn da was gestanden wäre, ich hätte es dennoch
140 angenommen oder bestätigt, daher.

141 A: Das heißt, wer kann das bestimmen, die Sicherheit deiner Fotos?

142 I: Die Firma von der App. Die das dann festlegen.

143 A: Die sagen dann, es ist gut geschützt oder nicht?

144 I: Wahrscheinlich ja.

145 A: Hast du da auch einen Einfluss darauf ob das gut geschützt ist oder nicht?

146 I: Wahrscheinlich bei Facebook kann man ja Einstellungen machen, wie gut man seine Daten
147 schützen möchte, ob das dann öffentlich wird oder nicht, bei den anderen Apps glaube ich
148 geht das nicht.

149 A: Und auf was deine Apps Zugriff haben, kannst du das einstellen?

150 I: Man kann halt ablehnen, aber dann nützt die gesamte App nichts, wahrscheinlich. Wenn ich
151 auf Instagram keine Fotos hochladen kann, dann nützt mir Instagram nichts.

152 A: Somit erhalten die Apps den Zugriff durch deine Zustimmung?

153 I: Ja.

154 A: Wieso meinst du, brauchen die Apps Zugriff auf mehrere, verschiedene Bereiche?

155 I: Weil sie mit anderen Bereichen agieren. Viele Apps kann ich ja nur in Verbindung mit
156 anderen Bereichen nutzen, zum Beispiel wie bei Instagram kann ich das nur mit Fotos nutzen
157 und so ist das auch sicher bei vielen anderen Apps der Fall. Zum Beispiel, dass ich eine App
158 nur in Verbindung mit der Musik nutzen kann, weil sie darauf zugreifen muss.

159 A: Wegen den Funktionen also, dass das überhaupt funktioniert?

160 I: Ja.

161 A: Hast du eine Musik App?

162 I: Ja. Musik App 1, die habe ich runtergeladen.

163 A: Jetzt sage ich dir wieder ein Beispiel: Kannst du dir vorstellen, dass die Musik App Zugriff
164 auf das Internet braucht, um funktionieren zu können?

165 I: Ja.

166 A: Wie sieht es aus, wenn sie sagt sie brauche Zugriff auf dein Adressbuch?

167 I: Wäre sicherlich nicht so sinnvoll. Aber könnte ich sicher auch ablehnen, aber ich würde
168 sicher ja sagen, weil ich meine, ich will die App ja auch in vollen Zügen genießen, ich möchte

169 ja alle Funktionen dabei haben. Das heißt, wenn ich da dann nein anklicke, dann würde eine
170 Funktion nicht funktionieren und dann wäre ich da auch nicht ganz zufrieden, denke ich.

171 A: Wieso meinst du braucht die App Zugriff auf das Adressbuch?

172 I: Damit ich vielleicht mit anderen Benutzern, die das auch haben, agieren kann, dass wenn
173 ich sehe, diese Nummer hat auch diese App auf dem Handy, dass man dann automatisch
174 befreundet ist, ihr folgt oder, dass diese eine Benachrichtigung bekommt, dass ich das auch
175 habe.

176 A: Kannst du dir vorstellen, welchen Grund die Firma oder die App hat, dass sie Funktionen
177 einbaut, bei denen sie auf das Adressbuch zugreifen müssen?

178 I: Wahrscheinlich um sämtliche Nummern zu bekommen, um E-Mail-Adressen zu
179 bekommen.

180 A: Was können sie machen mit diesen Adressen?

181 I: Werbungen schicken, verkaufen. Ich denke das ist der Hauptgrund.

182 A: Meinst du, gibt es noch einen Grund, dass Firmen das machen, außer Werbung?

183 I: Daten sind immer beliebt. Also ich denke unabhängig, ob das alles brauchbare Daten sind,
184 je mehr du hast, hast du halt viele.

185 A: Was kannst du mit diesen Daten machen, wenn du viele hast?

186 I: Gut, du kannst sie verkaufen, du kannst sie auch nur benutzen, um selbst Sachen
187 auszuschicken, um selbst Werbung zu machen, wahrscheinlich. Du kannst mit diesen Daten
188 viel anfangen, glaube ich.

189 A: Vor allem im Werbebereich jetzt?

190 I: Immer im Werbebereich, weil sonst bringt dir das ja nichts eigentlich. Ich glaube das ist
191 alles nur für den Werbebereich geeignet, dass du die Daten besitzt. Gleich ist es bei Firma 3,
192 wenn du viele Daten hast, umso mehr Newsletter kannst du rausschicken. Je mehr Daten du
193 hast, umso mehr Personen erreichst du. Das wird da das gleiche sein.

194 A: Was meinst du, wenn jetzt ein Unternehmen nicht nur von dir viele Daten besitzt, sondern
195 auch unzählig viele Daten von unzählig vielen anderen Leuten in verschiedenen Bereichen?
196 Was nutzt das diesem Unternehmen?

197 I: Macht, denke ich auch. Ich meine, wenn du weißt, ich habe jetzt von Millionen von Leuten
198 die Daten, ist das sicher auch etwas, was in der Konkurrenz auch mit Macht zu tun hat. Auch
199 mit Vorsprung, wenn du mehr Daten hast, wie andere. Ob das jetzt wirklich was bringt, weiß
200 ich auch nicht, aber ich denke schon. Also kann nicht schlecht sein, kann ja nur gut sein.

201 A: Macht ist sicher ein Punkt, aber die Macht muss ich ja ausnutzen, ich muss mit den Daten
202 ja auch irgendwas machen, damit es zur Macht wird. Hast du eine Vorstellung wie aus Daten
203 Macht wird?

204 I: Kaufen, verkaufen, Werbung.

205 A: Und was machen diese Unternehmen, die Daten kaufen?

206 Werbung schicken, denke ich mir mal.

207 A: Was kann das für uns welche Folgen haben, wenn ein Unternehmen all unsere Daten hat
208 und auch die von unzählig vielen anderen?

209 I: Also ich merke das bei mir bei meiner E-Mail-Adresse, dass ich nach einer gewissen Zeit
210 hunderte von E-Mails bekomme mit Werbungen, Werbungen, Werbungen, die nicht immer
211 im Spamordner fallen. Das ist sicher etwas, das negativ ist, das eher ein bisschen lästig ist,
212 wenn man sie selbst löschen muss. Das gleiche ist mit dem Handy, wenn du immer SMS
213 bekommst mit Werbung. Post kannst du auch bekommen, wenn du die Adresse angibst. Ja,
214 das ist das, das mich am meisten stört. Unabhängig von Kreditdaten oder so, nur mit Adressen
215 und sowas.

216 A: Und, wenn diese Daten jetzt analysiert werden, weil das müssen sie ja, wenn du eine
217 Werbung erstellen willst, ist es dann möglich, dass man bei der Auswertung schon
218 Besonderheiten aus den Daten sehen kann?

219 I: Das hängt davon ab, wenn du jetzt nur die Daten hast von einem Benutzer, der die App
220 benutzt, kannst du sicher eine gute Statistik machen. Aber wenn du jetzt wirklich alle
221 Adressen hernimmst, dann weißt du ja nicht wer was benützt. Also ich denke, wenn du jetzt
222 die Daten hernimmst von dem Benutzer, der die App benutzt, ist das sicher super, um
223 Statistiken zu erstellen, wo du auch sehen kannst wie viel Prozent der Nutzer zum Beispiel
224 männlich sind, wie viele weiblich, zum Beispiel. Aber wenn du jetzt wirklich alle Daten vom
225 Adressbuch nimmst, weiß ich nicht wie viel du damit erreichen kannst. Weil da hast du ja nur
226 die Daten, du weißt ja nicht, was diese verschiedenen Kontakte machen. Du weißt ja nur den
227 Kontakt.

228 A: Kannst du dir aber vorstellen, dass man das schon so genau zusammensuchen kann, dass
229 man sogar sagen kann, wer mit wem und wie und was zu tun hat?

230 I: Ah ja, sicher. Ich glaube, das sieht man auch bei Facebook. Wenn du reingehst, dass du
231 siehst wer mit wem befreundet ist, was derjenige macht usw.

232 A: Hast du dir schon mal überlegt, einen Dienst oder eine App deswegen aufzugeben, weil er
233 so viele Daten sich nimmt?

234 I: Nein, an das habe ich noch nie gedacht.

235 A: Du hast aber gesagt, du hast relativ wenige Apps installiert. Ist da unter anderem ein
236 Grund, weil du sagst ich möchte nicht zu viel von mir preisgeben? Also die wichtigen Apps
237 wie Facebook und WhatsApp und so, installiere ich, weil sie mir einen Nutzen bringen, aber
238 die anderen installiere ich nicht, weil im Grunde nehmen sie sich viele Daten und ich habe
239 keinen Nutzen davon?

240 I: Ja es ist halt einfach, weil der Sinn ist ja nicht, dass ich hunderte von Apps drauf habe, also
241 nicht wegen meinen Daten, sondern damit kein Chaos auf meinem Smartphone herrscht,
242 damit es ein wenig geordnet ist. Aber der Grund ist sicher nicht, dass ich meine Daten sichern
243 möchte.

244 A: Was müsste zum Beispiel passieren, dass du wirklich sagst, diese App lösche ich?

245 I: Hm, viel müsste da passieren. Dass vor allem meine Fotos, meine Chats alle online gestellt
246 werden. Aber ich meine, auch wenn das passieren würde, wer sieht sich das an? Wenn jetzt
247 wirklich tausende Chats online gestellt werden, das interessiert ja keinen, von normalen
248 Leuten.

249 A: Was ist, wenn du später einmal bekannt bist?

250 I: Ja, ich meine jetzt schon normale Leute, jetzt wie zum Beispiel bei den Promis, wo die
251 vielen Nacktbilder veröffentlicht wurden, das ist dann sicher eine andere Sache, weil diese
252 kennt man, da weiß man, dass es diese Personen gibt. Aber bei den normalen Leuten, glaube
253 ich, interessiert das nicht viele, ob jetzt die Person XY ein Problem hat.

254 A: Wenn jetzt von dir alle Chats online wären, dann würdest du aber schon sagen, das geht
255 jetzt zu weit?

256 I: Ja, wenn man wirklich kann spezifisch danach suchen. Wenn ich meinen Namen eingeben
257 kann und dann alles aufgelistet wird, alle Daten von mir halt, wenn du wirklich mit dem
258 Namen nach solchen Sachen suchen könntest, dann schon.

259 A: Wenn deine Privatsphäre verletzt wird.

260 I: Genau. Wenn jetzt hunderte von Chats in einen Topf geschmissen werden, alle drunter und
261 drüber gemischt, dann ist das was anderes. Dann findet mich keiner mehr, der mich kennt.
262 Hoffe ich mal.

263 A: Mit Gesichtserkennung vielleicht?

264 I: Habe ich auch kein Problem damit.

265 A: Wie möchtest du dich in Zukunft vor Datenraub oder –Speicherung schützen?

266 I: Also ich meine in Zukunft, wenn ich arbeite und wichtigere Daten habe, Dokumente, Pläne,
267 was weiß ich was, da will ich dann schon ein bisschen besser darauf aufpassen. Aber jetzt im
268 Moment mit meinen privaten Fotos, da ist nichts Wichtiges, Interessantes dabei wo man

269 wirklich sagen könnte, dass eine Konkurrenz etwas damit anfangen könnte, also nur von
270 normalen Personen.

271 A: Also Daten von normalen Personen siehst du nicht als wertvoll an?

272 I: Nein, sehe ich nicht als wertvoll. Das sehe ich als uninteressant. Also vielleicht in Zukunft,
273 wenn ich wirklich Daten von bestimmten Personen habe, dann werde ich sicherlich Acht
274 geben müssen, dass ich besser darauf aufpasse. Dann werde ich das aber bestimmt nicht auf
275 dem Handy irgendwo haben, sondern auf dem Server irgendwo gesichert. Da mache ich mir
276 weniger Sorgen.

277 A: Wie denkst du wird unser Leben mit dieser Technologie in 30, 50 Jahren aussehen?

278 I: Kompliziert, oder einfach, je nachdem, wenn wir wissen, wie es dahinter aussieht, einfach,
279 aber ich denke für uns alle kompliziert. Aber ich denke auch nicht recht viel anders als jetzt,
280 kann ich mir vorstellen. Das Prinzip ist ja schon da. Das Prinzip wird sich auch nicht
281 großartig ändern, man kann ja die Welt nicht völlig neu erfinden. Handys werden Handys
282 bleiben, vielleicht ein bisschen dünner, ein bisschen flacher, keine Ahnung, was sich halt
283 ändert, aber das Prinzip wird das selbe sein.

284 A: Und das Prinzip ist so, dass fast jeder ein Handy besitzt?

285 I: Hat eigentlich fast jeder eines. Vielleicht irgendwas mit einem Chip oder so was. Aber das
286 mit dem Chip kann ich mir auch schlecht vorstellen, dass das die Leute machen, sich etwas
287 einpflanzen lassen, außer es wird cool, ich weiß nicht, wenn es Trend wird. Aber ich denke in
288 30 Jahren haben wir schon noch Handys.

289 A: Ok, und jeder ist mit jedem verbunden, sozusagen?

290 I: Ja, das in jedem Fall.

291 A: Gut, ich schildere dir jetzt ein paar Beispiele und frage dich ob du diese für realistisch
292 hältst oder nicht und warum.

293 Wenn jemand täglich das Smartphone mit Apps und Internet zum Beispiel Twitter und/oder
294 Facebook nützt, aber niemals seinen Standort preisgibt. Wäre es für dich dann vorstellbar,
295 dass man mit großer Wahrscheinlichkeit vorhersagen kann, wo sich derjenige in Zukunft
296 aufhalten wird?

297 I: Sicher! Wenn du die Gewohnheiten von diesem Menschen kennst, wenn du weißt er ist
298 jeden Mittwoch, ein Foto vom Fitnessstudio postet, auch wenn er den Standort jetzt nicht
299 dazuschreibt, dass er mittwochs um diese Zeit im Fitnessstudio ist. Also ich glaube, das ist
300 schon der Fall.

301 A: Wieso ist es wahrscheinlich, dass er das wieder macht?

302 I: Ja, ich denke mir, wenn du das über mehrere Wochen lang so machst, dann wirst du das
303 auch in Zukunft beibehalten.

304 A: Nehmen wir mal an, diese Personen postet keine Fotos oder sonst was, und hätte zum
305 Beispiel auch ihr Handy verloren, kannst du dir vorstellen, dass man nur durch ein paar enge
306 Freunde von Facebook zum Beispiel doch den Standort der anderen Person herausfinden
307 kann? Und diese Freunde posten nicht, dass sie mit der gesuchten Person an einem
308 bestimmten Ort sind.

309 I: Jaja, ich denke man hat vielleicht – nein das ist schwierig glaube ich. Also ich glaube man
310 könnte vielleicht sagen, diese Person könnte vielleicht da oder dort sein, aber ich glaube
311 richtig rausfinden, kann man das auch nicht.

312 A: Mit Wahrscheinlichkeit vorhersagen dann aber schon?

313 I: Ein Ratespiel ist das dann wahrscheinlich.

314 A: Eher sicher oder eher ungenau?

315 I: Eher ungenau denke ich mir.

316 A: Was ist für dich eher ungenau in Prozent ungefähr?

317 I: Ich sage diese Person ist vielleicht beim Training, weil sie immer trainiert, mit 20 Prozent
318 Wahrscheinlichkeit. Wer weiß, dass ich oft trainiere, wird mich mit hoher Wahrscheinlichkeit
319 am Trainingsplatz vorfinden.

320 A: Hast du schon einmal davon gehört?

321 I: Nein.

322 A: Wie realistisch ist es für dich, dass die Polizei bereits heute wissen kann, wo morgen ein
323 Verbrechen stattfindet?

324 I: Sehr realistisch. Ich meine, wenn jemand dahinter ist und wirklich Chats und Verläufe
325 ansieht, dann kann ich mir schon vorstellen, dass das realistisch ist. Ich meine, es ist ja schon
326 Realität, dass das praktiziert wird.

327 A: Kannst du dir auch vorstellen, dass, wenn die Polizei keinen Verdächtigen überwacht, das
328 sie dennoch sagen kann mit einer gewissen Wahrscheinlichkeit ist bei Ort A etwas, mit einer
329 gewissen Wahrscheinlichkeit ist an Ort B etwas.

330 I: Ja sicher mit Postings.

331 A: Und wenn sie zum Beispiel darauf achtet, wo früher Verbrechen stattfanden?

332 I: Statistisch meinst du? Ja, aber ich glaube das ist auch eine schwierige Sache. Also, sicher in
333 einem kleinen Ort bringt dir eine Statistik auch nichts, wenn da vor zehn Jahren was passiert
334 ist, dann wird da nicht wieder was passieren, kann ich mir vorstellen, wenn man eine große
335 Masse oder ein großes Gebiet ansieht, dann vielleicht.

336 A: Wenn wir eine Großstadt hernehmen zum Beispiel?

337 I: Da ist es sicher anders, wenn du weißt an diesem Tag ist ein super-schlechtes Wetter,
338 vielleicht sind da mehr Kriminelle unterwegs, weil sie alle in den Häusern bleiben, die
339 Verkäufer in den Geschäften oft alleine, die Polizei sonst schon alle Hände voll zu tun hat,
340 vielleicht kann man dann statistisch sagen, dass bei großen Unwettern die Wahrscheinlichkeit
341 für Einbrüche in Geschäfte oder Lokale höher ist. Aber sonst eigentlich, denk ich mir nicht.

342 A: Aber jetzt den Ort halbwegs zu bestimmen, das denkst du, ist nicht möglich?

343 I: Sicher, wenn ein bisschen mehr Kriminalität in diesem Ort herrscht, dann kannst du davon
344 ausgehen, dass das passieren könnte. Wie an einem Ort, wo alles nur alte Leute wohnen und
345 keiner macht was und keiner hat etwas.

346 A: Das heißt, wie machen sie das, wie finden sie das heraus?

347 I: Durch Statistiken. Wenn sie sehen, da passiert was, dann wird es wieder da passieren
348 wahrscheinlich. Oder ist die höhere Wahrscheinlichkeit, dass es dort passiert, als an einem
349 anderen Ort.

350 A: Hast du davon schon mal gehört?

351 I: Nein.

352 A: Nehmen wir an eine Frau kauft im Supermarkt verschiedene Sachen ein, jedoch keinerlei
353 Babysachen. Kannst du dir vorstellen, dass man nur aus den gekauften Artikeln mit hoher
354 Wahrscheinlichkeit sagen kann, ob diese Frau schwanger ist oder auch nicht und ungefähr ob
355 sie sich in der frühen, mittleren oder späten Schwangerschaft befindet?

356 I: Ich denke, wenn sie einen Schwangerschaftstest kauft, ist die Möglichkeit hoch, dass sie
357 schwanger sein könnte und dann wird sie in der frühen Schwangerschaft sein, aber das ist
358 offensichtlich dann. Sicher, wenn du einen Kinderwagen kaufst, dann wird es schon eher nahe
359 dem Ende der Schwangerschaft sein.

360 A: Und was ist, wenn sie keine Sachen kauft, die man mit Kindern oder Babys in Verbindung
361 bringt?

362 I: Gar keine? Ich kenn mich bei Schwangeren nicht aus, ich weiß nicht was diese essen, aber
363 vielleicht, wenn sie wirklich, wenn man sieht, dass im Durchschnitt eine schwangere Frau
364 bestimmte Vorlieben für ein paar Produkte hat, dann kannst du dir sicher vorstellen, dass sie
365 vielleicht schwanger sein könnte, aber sonst, also ich würde das nicht sagen können.

366 A: Aber du kannst es dir vorstellen, dass man das vorhersagen kann?

367 I: Ja, wenn sich da jemand wirklich gut auskennt und weiß, was eine Schwangere normal
368 einkauft und essen tut, ich glaube im Gesamten sind sie sich alle ein bisschen ähnlich,
369 deshalb, wenn man sich auskennt, kann man das sicher bestimmen.

370 A: Das funktioniert dann wie?

371 I: Auf lange Zeit sicher viele Frauen kontrollieren, welches Verhalten sie beim Einkaufen
372 haben.

373 A: Das heißt eigentlich kannst du dir vorstellen, dass man vorhersagen kann, ob sie
374 schwanger ist oder nicht. Wie sieht es mit dem Anfang, Mitte oder Ende der Schwangerschaft
375 aus? Kann man das auch sagen?

376 I: Also, man sieht wahrscheinlich am Ende, dass sie einen großen Bauch hat, aber nur an den
377 Artikeln? Ja, bestimmt, eine Hochschwangere kauft sicher andere Sachen, wie eine die nicht
378 schwanger ist. Aber ich würde das jetzt nicht wissen. Ich bin der Meinung, es geht sicher,
379 aber dazu muss man sich halt auskennen. Welche Artikel oder wie man das herausfinden
380 kann, könnte ich jetzt nicht sagen.

381 A: Hast du schon einmal davon gehört?

382 I: Nein, eigentlich nicht.

383 A: Nehmen wir an, ein Mann ist homosexuell, er nützt das Internet, darunter auch Social
384 Media, gibt jedoch nirgends an, dass er Männer liebt. Sein Sexualleben wird von ihm auch
385 geheim gehalten und er gibt es weder im Internet noch sonst irgendwo preis. Für wie
386 realistisch haltest du es, dass wildfremde Personen dennoch mit hoher Wahrscheinlichkeit
387 sagen können, dass der Mann homosexuell ist?

388 I: Also ich glaube mal, man sieht es auch an den Fotos, wenn er es erkenntlich macht,
389 ansonsten sicher bei den Posts, ich meine Homosexuelle posten sicher anderes als
390 Heterosexuelle, oder auch in einem anderen Stil, meine ich mal. Oder auch die Vorlieben von
391 den Seiten, die er liked, wenn einem was Gott was gefällt, was mehr fraulich, sag ich jetzt
392 mal, ist, wie Handtaschen liken oder ich weiß es nicht, dann ist das sicher etwas wo man sich
393 das denken könnte. Ich weiß es nicht. Aber ich meine das ist dann immer nur Spekulation,
394 genau sagen kann man es nicht, weil ich meine heutzutage geht ja alles.

395 A: Nein, genau, dass man etwas mit 100% Wahrscheinlichkeit sagen kann, ist nicht gemeint.

396 I: Ich bin sicher der Meinung, dass man es sich vorstellen kann, dass ein Mann vielleicht
397 homosexuell sein könnte, aber es eigentlich nicht ist. Ganz ehrlich. Ich kann mir vorstellen,
398 dass andere, die komplett andere Sachen geliked haben, auch homosexuell sein können. Aber
399 ich weiß es nicht, schwierig. Da ist das Beispiel mit der Schwangeren schon fast realistischer
400 für mich, wenn er es geheim hält.

401 A: Wieso hältst du es für realistisch, dass man es beim homosexuellen Mann, wenn er es
402 geheim hält, nicht erkennt?

403 I: Ja weil er es geheim hält, die Schwangere versucht ja nicht, nicht schwanger zu sein. Weil
404 wenn jemand das geheim halten will, dann liked er extra nicht diese Seite, dann stellt er extra
405 nicht dieses Bild rein.

406 A: Kannst du dir vorstellen, dass es auch andere Faktoren gibt, die er nicht einmal bedenkt,
407 also nicht typisch homosexuelle Faktoren, sondern vielleicht ganz andere, alltägliche
408 Faktoren, wo aber die Häufigkeit bei homosexuellen Männern sehr hoch ist? Und wenn
409 jemand mehrere von diesen Faktoren hat, dass dann die Wahrscheinlichkeit größer ist, dass er
410 homosexuell ist.

411 I: Ich glaube schon, aber jetzt nur auf Facebook und solche Medien bezogen, ist es halt
412 dennoch schwierig, wenn man es wirklich geheim hält, dass man es herausfindet, aber sonst
413 im Leben sieht man oder merkt man ja, ob jemand eher schwul ist.

414 A: Ok. Hast du schon einmal davon gehört?

415 I: Nein, nicht bewusst glaube ich.

416 A: Kannst du dir vorstellen, dass Kreditinstitute in Zukunft deine Freundesliste auf Facebook
417 kontrollieren und auch die Bewegungsdaten von deinem Smartphone heranziehen, wenn sie
418 prüfen wollen, ob du kreditwürdig bist oder nicht und welchen Kredit du bekommst?

419 I: Bestimmt! Also ich bin mir relativ sicher.

420 A: Wieso?

421 I: Ja, weil man will sich ja relativ absichern, das gleiche ist in anderen Betrieben. Wenn du
422 wirklich jemanden anstellen willst, dann schaust du ja auch auf Facebook nach. Auch wenn
423 man es nicht machen sollte, aber man will ja doch wissen, was macht der. Ist der immer nur
424 beim Party machen, wirft der nur das Geld vom Fenster, man sieht ja, ob er bewusst mit dem
425 Geld auch umgeht. Und wenn du jetzt ein Kreditinstitut bist und du siehst, dass diese Person
426 immer nur Party macht und das Geld beim Fenster rauswirft, überlegst du es dir zwei Mal.
427 Wenn du siehst, diese Person macht viel Sport, und macht normalere Sachen, bewusstere
428 Sachen, dann ist das anders.

429 A: Das heißt du hast davon schon gehört?

430 I: Ich habe jetzt nicht davon gehört, aber ich bin mir sicher, relativ, dass es so ablaufen wird,
431 dass es so kontrolliert wird bei Privatpersonen mal.

432 A: Kennst du die Gesundheits- und Fitnessapp's, die man am Smartphone herunterladen
433 kann?

434 I: Gehört habe ich davon, aber ich kenne keine.

435 A: Aber du weißt was ich meine.

436 I: Ich weiß, dass es diese gibt, ja.

437 A: Kannst du dir vorstellen, dass in Zukunft Gesundheitsversicherungen sich mit solchen
438 Apps zusammenschließen, wenn sie prüfen wollen, ob du regelmäßig Sport machst und ob du
439 dich gesund ernährst, wenn sie entscheiden wollen ob du eine Versicherung bekommst oder
440 nicht?

441 I: Das wäre böse! Ich glaube, nein ich glaube das würde man nicht zulassen.

442 A: Wer?

443 I: Wir als Konsumenten. Ich glaube die würden sicher sagen, nein, ich möchte jetzt nicht, dass
444 meine Versicherung, dass ich wirklich Sport machen muss, damit ich die Versicherung
445 bekomme, oder billiger oder zu besseren Konditionen. Ich glaube, da würde keiner
446 mitspielen, da würde es schon einen Protest geben. Aber ich kann mir vorstellen, dass es für
447 die Versicherung, es wäre halt, ja schwierig, aber ich glaube das würde sich nicht
448 durchsetzen, das kann ich mir nicht vorstellen. Weil wir als Konsumenten nicht mitspielen.
449 Nur wegen dem.

450 A: Aber im Grunde, wenn es günstiger wird, machen ja dennoch viele Leute mit, weil sie
451 denken, dass sie dabei ein Schnäppchen machen.

452 I: Ja, aber es ist halt doch. Wenn jemand nichts macht und er dennoch die Versicherung
453 braucht, ich meine, auf die Masse gesehen, viele machen ja gar nichts und auf die Masse
454 gesehen machen wenige Leute Sport, deswegen, glaube ich, würde sich das nie durchsetzen.

455 A: Hast du schon einmal davon gehört?

456 I: Nein.

457 A: Wie wahrscheinlich hältst du das Szenario, dass man in Zukunft in ein Land zum Beispiel
458 nicht mehr einreisen darf, weil man ein bestimmtes Wort im Internet eingegeben hat oder in
459 einer SMS geschrieben hat?

460 I: Schwierig, je nachdem in welches Land, weil wenn du jetzt, sicher. Ja, aber ich glaube nicht
461 dass das jetzt, ja, wenn es wirklich kontrolliert wird? Und du wirklich willst in dieses Land
462 einreisen, und zum Beispiel Russland kontrolliert, und du in Russland einreisen willst und
463 Russland sieht, dass du homosexuell bist, dann wollen wir dich nicht, ich glaube das ist
464 sicher. Ja, wenn sich wirklich jemand den Kopf macht und sagt, ich will das alles
465 kontrollieren, wer in mein Land kommt, dann schon, denke ich. Ich glaube das ist schon
466 realistisch.

467 A: Kannst du dir vorstellen, dass Russland, USA, Korea und solche Staaten zum Beispiel
468 wirklich kontrollieren, wer in ihr Land einreist?

469 I: Ja ich denke schon. Ja, es ist schwierig, weil ich weiß jetzt nicht, wie viele wirklich
470 einreisen und was das welcher Aufwand ist, das alles zu kontrollieren. Aber so rein
471 theoretisch finde ich, ist das schon was, was sie machen würden.

472 A: Also wenn die technischen Möglichkeiten gegeben sind, dann schon?

473 I: Man will ja wissen ob das ein Terrorist ist oder nicht.

474 A: Wenn wir zwei in die USA fliegen würden und ich dir vorher schreiben würde, wir werden
475 uns in Amerika zerstören, meinen damit, dass wir uns mit Alkohol zerstören werden, könntest
476 du dir vorstellen, dass wir dann Probleme bekommen bei der Einreise?

477 I: Also ich glaube nur so kurzfristig geht das nicht. Also, wenn ich jetzt nur einreise, um
478 Urlaub zu machen ein paar Monate, dann kann ich mir nicht vorstellen, dass das alles
479 kontrolliert wird, das wäre ein zu großer Aufwand. Aber wenn ich wirklich Staatsbürgerschaft
480 wechseln will und zum Beispiel die amerikanische Staatsbürgerschaft beantrage, dann kann
481 ich mir vorstellen, dass sie wirklich an dem Tag, an dem ich den Antrag zur Umsiedlung
482 stelle, dass da schon etwas kontrolliert wird. Aber ich meine, wenn das wirklich nur ein
483 Urlaub ist, oder auch ein Jahr, dann wäre das ein zu großer Aufwand das zu kontrollieren.
484 Außer es ist ein mathematisches Programm, das alles durchsucht, aber das kann ich mir nicht
485 vorstellen. Da würden auch nur Missverständnisse rauskommen, wahrscheinlich. Deswegen:
486 Kurzfristig gesehen, wenn man nur kurzfristig einreist, ist da nichts, von mir aus gesehen. Das
487 wäre meiner Meinung zu aufwändig.

488 A: Hast du schon einmal davon gehört?

489 I: Nein.

490 A: Gut, dann das letzte Beispiel: Ist es für dich realistisch, dass man aus dem Verhalten der
491 Vergangenheit, das Verhalten in der Zukunft schon vorhersagen kann mit einer gewissen
492 Wahrscheinlichkeit?

493 I: Ja! Also ich denke, wenn ich immer viel esse, dann kann ich mir vorstellen, dass ich mit 40
494 Jahren immer noch viel esse und vielleicht halt ein wenig dicker bin. Also ich denke, das ist
495 etwas, was logisch ist. Dass sich der Mensch nicht in allen Bereichen ändern wird in seinem
496 Leben, dass ein gewisses Grundverhalten immer da sein wird. Eine gewisse Linie wird immer
497 gleich bleiben, denke ich.

498 A: Danke für das Interview.

16.4. Beispiel Kategoriensystem

Kategorie 1: Datenanalyse			
Extraktion	Aufbereitung	Auswertung	Stichwörter
Auswertungseinheit 1			
A: Du hast ja gesagt, für Werbung. Aber wieso verkaufen sie deine Daten an andere Unternehmen? I: Ja für Geld, damit sie Geld bekommen. (Z 169-171)	wieso verkaufen sie deine Daten? damit sie Geld bekommen. (Z 169-171)	Eigene Daten werden an andere Unternehmen für Geld verkauft. (Z 169-171)	Daten für Geld verkauft. Werbung.
A: Was machen dann die anderen Unternehmen mit deinen Daten? I: Werbungen und solche Sachen, denk ich mir. (Z 172-173)	andere Unternehmen machen Werbung. (Z 172-173)	Unternehmen nutzen Daten für Werbung. (Z172-173)	Werbung.
A: Was, meinst du, können Unternehmen machen, wenn sie unzählig viele Daten von dir haben? Und nicht nur von dir, sondern von unzählig vielen andern Leuten. Gibt es noch einen anderen Gedanken außer Werbung? I: Sicher, wenn sie Passwörter von Internetseiten oder Kreditkarten haben. Aber das mache ich nicht über das Handy. Vielleicht erpressen sie dich auch. Aber das glaube ich nicht. Was sie sonst noch machen könnten mit diesen Daten? Ich wüsste es nicht. (Z 174-179)	wenn sie Passwörter von Internetseiten oder Kreditkarten haben. Vielleicht erpressen sie dich. Glaube ich nicht. Was sie sonst noch machen? Ich wüsste es nicht. (Z 174-179)	Die Person ist unsicher, kann sich aber vorstellen, dass eine Erpressung eine Folge des Datenzugriffes sein kann. Andere Vorstellungen werden nicht geäußert. (Z 174-179)	Unsicherheit. Erpressung.

Auswertungseinheit 2			
A: Du hast ja gesagt, dass diese Unternehmen die Daten weiterverkaufen. Was können denn Apps machen, wenn sie Zugriff auf deine Fotos, dein Adressbuch u.s. w. haben. Was nutzt ihnen das? I: Damit sie die Werbung auf jemanden genau zuschneiden können. Dass sie genau wissen, zum Beispiel mir gefällt Thema 1, weil ich alles bei Thema 1 like, dass sie dann genau wissen wie sie die Werbung zuschneiden müssen. A: Kannst du dir noch was vorstellen, außer Werbung? I: Weiterverkaufen, aber was dann genau... (Z136-143)	Werbung auf jemanden genau zuschneiden. Weiterverkaufen. (Z136-143)	Der Zugriff auf Fotos und Adressbuch nützt den Unternehmen, damit sie Werbung auf die Person gezielt zuschneiden können und Daten weiterverkaufen können. (Z136-143)	Werbung. Daten weiterverkaufen.
A: Was machen Firmen zum Beispiel, die Daten kaufen? I: Die kaufen Daten und verkaufen diese dann natürlich auch weiter, damit sie die Werbung optimieren können und sie genau auf die Leute zuschneiden können. A: Und diese Firmen, die interessiert sind an diesen Daten, was machen diese dann damit? I: Weiterverwenden um zu kontrollieren, was sie verbessern können an ihren Produkten und so. A: Welchen Nutzen, außer Werbung, können Unternehmen noch aus Daten ziehen? I: Das wüsste ich jetzt nicht. (Z144-151)	kaufen Daten und verkaufen diese dann weiter, damit sie die Werbung optimieren können, genau auf die Leute zuschneiden können. kontrollieren, was sie verbessern können an ihren Produkten. Außer Werbung keine Idee, was Firmen machen können mit Daten. (Z144-151)	Der Nutzer weiß, dass Firmen Daten nutzen, um Werbung zu personalisieren und Produkte zu verbessern. Er kann sich jedoch keinen andern Nutzen, außer für Werbung, vorstellen. (Z144-151)	Werbung. Verbesserung der Produkte.
A: Wenn du dir vorstellst ein Unternehmen hat unzählig viele Daten von vielen Leuten. Was können diese dann damit tun? I: Ja, zum einen weiterverkaufen an andere Firmen, zum anderen, wenn sie selbst Produkte haben, für sich selbst nutzen. Ja, in diesen Bereich denk ich mir. (Z 152-155)	Unternehmen mit unzählig vielen Daten kann diese weiterverkaufen, oder selbst nutzen, um Produkte zu verbessern. (Z 152-155)	Es besteht das Wissen, dass Unternehmen, welche im Besitz von vielen Daten sind, diese für eigene Zwecke, wie jenem der Produktverbesserung, verwenden, aber sie können die Daten auch an andere Unternehmen weiterverkaufen. (Z 152-155)	Daten weiterverkaufen. Verbesserung der Produkte.

A: Welche Folgen hat das dann für uns? I: Dass wir weniger Privatsphäre haben (...?). A: Was bedeutet für dich Privatsphäre? I: Dass meine eigenen Sachen geschützt sind vor anderen, dass ich es nur selbst sehe, außer ich will es anderen zeigen. (Z 156-160)	Folgen für uns: Dass wir weniger Privatsphäre haben. Dass meine eigenen Sachen geschützt sind vor anderen, dass ich es nur selbst sehe, außer ich will es anderen zeigen. (Z 156-160)	Die Folgen, die sich für uns daraus ergeben, sind ein Einschnitt in unsere Privatsphäre. Privatsphäre wird gleichgesetzt mit dem Schutz eigener Dateien vor der ungewollten Einsichtnahme anderer. (Z 156-160)	Weniger Privatsphäre.
A: Nehmen wir mal an, der Max ladet sich eine App runter und akzeptiert bei der Installation, dass die App Zugriff hat auf seine Fotos, sein Adressbuch, sein Kalender und all diese Sachen. Die App speichert alle Informationen, also die ganzen Fotos, alle Nummern, die er im Adressbuch hat. Was meinst du: Wie könnte das für den Max dann aussehen, wenn die Firma all seine Daten hat? I: Dann sieht die Firma genau, was der Max alles tut, was ihn interessiert, wer seine Freunde sind und so. A: Und was kann die Firma dann machen, wenn sie alles über den Max weiß? I: ... sie kann ihm Werbung zuschicken, die sie genau auf ihn angepasst, damit er ja kauft. ... sie könnte ihn erpressen, aber nein, das würde sie wohl eher nicht tun. Ja. (Z 161-170)	Dann sieht die Firma genau, was der Max alles tut, was ihn interessiert, wer seine Freunde sind. Kann Werbung genau auf ihn anpassen, erpressen unwahrscheinlich. (Z 161-170)	Folgen von Datenspeicherung und -Sammlung durch Firmen: Firmen wissen genau, welches Verhalten und welche Interessen wir haben. Möglichkeit der angepassten Werbung. Unwahrscheinlich: Erpressung. (Z 161-170)	Werbung. Erpressung unwahrscheinlich.
Auswertungseinheit 3			
A: Und was macht der im Hintergrund mit diesen Daten dann? I: Keine Ahnung. (lacht). Jetzt wenn ein Telefonbuch oder Adressbuch von jemand anderem genommen wird, ist logisch jetzt nicht soo, weil immerhin eine Handynummer ist etwas, das ich nicht hergebe. Also das ist bei mir auch nirgends drinnen. Also das ist. (Z181-184)	Was macht jemand mit deinen Daten? Keine Ahnung. Jetzt wenn ein Telefonbuch oder Adressbuch von jemand anderem genommen wird, ist logisch jetzt nicht soo. Eine Handynummer ist etwas, das ich nicht hergebe. (Z181-184)	Person weiß nicht, was eine andere Person mit ihren Daten machen kann. Es wäre ihr zwar unangenehm, sie schützt Handynummern auch, aber sie kann nicht sagen, was es einer anderen Person welchen Nutzen bringen kann. (Z181-184)	Weiß es nicht.

A: Du hast ja gesagt, dass die App Informationen kopiert und speichert. Was meinst du, kann ein Unternehmen machen, wenn es von unzählig vielen Leuten ganz, ganz viele Daten hat? I: Was sie damit machen? A: Ja. I: Jetzt, ausnutzen, ich weiß nicht, was sie damit machen können. Überprüfen, ja bo, das nützt ihnen ja auch nicht viel, wenn sie diese haben, was sollen sie mit denen? (Z185-190)	Was meinst du, kann ein Unternehmen machen, wenn es von unzählig vielen Leuten ganz, ganz viele Daten hat? ausnutzen, ich weiß nicht, was sie damit machen können. Überprüfen, das nützt ihnen ja auch nicht viel, wenn sie diese haben, was sollen sie mit denen? (Z185-190)	Person weiß nicht, welchen Nutzen Unternehmen aus vielen Daten ziehen können und was sie damit machen können. Es ist zwar das Bewusstsein vorhanden, dass Daten vom eigenen Smartphone gespeichert werden, aber es fehlt das Wissen, welchen Nutzen andere aus diese Daten ziehen können. (Z185-190)	Ausnützen. Unsicherheit.
A: Und welche Folgen könnte das für uns haben? I: Dass wir überhaupt keine Privatsphäre mehr haben, dass wir immer überwacht werden, also immer kontrolliert werden können wo wir sind und was wir machen. Und dass sie dann, der nächste Schritt ist dann, dass es bis zu Bankdaten, Kreditkarteninformationen und Handynummern dann auch nicht mehr weit ist, dass man halt überhaupt nichts mehr schützen kann, dass man eigentlich ein offenes Buch ist. (Z 191-196)	Welche Folgen für uns? Dass wir überhaupt keine Privatsphäre mehr haben, dass wir immer überwacht werden, also immer kontrolliert werden können wo wir sind und was wir machen. der nächste Schritt ist dann, dass es bis zu Bankdaten, Kreditkarteninformationen und Handynummern dann auch nicht mehr weit ist, dass man halt überhaupt nichts mehr schützen kann, dass man eigentlich ein offenes Buch ist. (Z 191-196)	Person weiß, dass die Folgen für uns darin bestehen, dass wir keine Privatsphäre mehr haben und immer überwacht und kontrolliert werden, wo wir sind und was wir machen. Sie schildert, dass es soweit gehen wird, dass wir auch Bankdaten, Kreditkarten und Handynummern, überhaupt nichts mehr schützen können und zu einem offenen Buch werden. (Z 191-196)	Überprüfung. Weniger Privatsphäre.

A: Nehmen wir mal an, die Anna ladet sich eine App runter und akzeptiert bei der Installation, dass die App überall zugreifen kann, auf Fotos, Adressbuch, Kalender und alles weitere. Die App speichert dann alle Informationen, welche die Anna auf ihrem Smartphone hat. Was meinst du: Welche Folgen könnte das für die Anna haben, wenn die App jetzt alles weiß. Alles, also die Daten, die sie auf dem Handy hat, sehen kann? I: Ja, angenehm ist das natürlich nicht. Folgen, ja eben überwacht sein, dass man nicht mehr das tun kann, was man eigentlich will, jetzt in der Hinsicht, dass zum Beispiel, wenn man eine SMS schreibt, möchte man, dass das nur unter zwei Personen bleibt und nicht dass zehn andere mitlesen. Die Privatsphäre, die man sich eigentlich wünscht, dass nicht alles öffentlich ist, dass diese wirklich öffentlich gemacht werden kann. (Z 197-206)	Welche Folgen wenn die App alles, alle Daten auf dem Handy sehen kann? angenehm ist das natürlich nicht. Folgen, überwacht sein, dass man nicht mehr das tun kann, was man eigentlich will, zum Beispiel, wenn man SMS schreibt, möchte man, dass das nur unter zwei Personen bleibt und nicht zehn andere mitlesen. Die Privatsphäre, die man sich eigentlich wünscht, dass nicht alles öffentlich ist, dass diese wirklich öffentlich gemacht werden kann. (Z 197-206)	Person weiß, dass die Folgen aus dieser Datenspeicherung unangenehm sind und man ständig überwacht wird und nicht mehr ungezwungen das tun kann, was man eigentlich möchte. Sie nennt auch den großen Einschnitt in die Privatsphäre mit der Überwachung der Kommunikation. Dass bei allem, bei dem man wünscht, dass es nicht öffentlich wird, die Möglichkeit besteht, dass es öffentlich gemacht werden kann. (Z 197-206)	Überwachung. Unangenehm. Anderes Verhalten durch weniger Privatsphäre.
---	---	---	---

A: Könntest du dir vorstellen, dass man sich dann anders verhält, wenn man weiß, da lest jemand mit? I: Ja, das denke ich schon. A: Ist das für dich ein Einschnitt in deine Privatsphäre und in dein Verhalten? I: Ja! Also wenn ich jetzt wüsste, dass andere mitlesen, was wahrscheinlich so ist, zum Beispiel bei Facebook, da weiß ich ja, das das so ist, dann ist das schon anders, ja. A: Wie verhältest du dich dann? I: Ja jetzt, eher, ich tu dann weniger posten oder, ich bin grundsätzlich nicht jemand der alles reinstellt, also Fotos schon aber ich mag zum Beispiel nicht, wenn man schreibt wo man gerade ist. Das mag ich überhaupt nicht, dass jeder weiß wo ich gerade bin, das kann man ja eingeben mit dem Standort und so. Handynummer würde ich auch nie reinstellen, wobei mir schon die E-Mailadresse eigentlich schon zu viel ist, aber die ist, ja., Eben, wenn man sich anmeldet, denkt man oft nicht an die Sachen. (Z 207- 219)	Denke ich schon, dass man sich anders verhält. Das ist Einschnitt in meine Privatsphäre und in mein Verhalten. Wenn ich weiß, da lesen andere mit, was ja so ist, dann ist das schon anders. Ich tue dann weniger posten, mag nicht, wenn man alles reinstellt, wo man ist, das mag ich überhaupt nicht. E-Mailadresse schon zu viel, an das denkt man nicht, wenn man sich anmeldet. (Z 207- 219)	Person ist überzeugt, dass man sich anders verhält, wenn man weiß, dass man beobachtet oder überwacht wird. Es ist für sie ein Einschnitt in die Privatsphäre und in ihr Verhalten. Sie mag es nicht, wenn andere wissen was sie macht und wo sie gerade ist. Persönliche Daten vermeidet sie, aber sie sagt, an die Folgen denkt man nicht, wenn man sich bei einem Dienst anmeldet. . (Z 207- 219)	Einschnitt in Privatsphäre. Anderes Verhalten. Oft nicht bewusst.
---	---	---	--

Auswertungseinheit 4			
A: Was nützt diesen Unternehmen eigentlich die Daten, wenn sie von dir das Adressbuch haben, die Kalendernotizen. I: Ja, da können sie Werbung machen, da können sie Umsatz machen. Ja, ich denk mir für das sicher. A: Vorwiegend einfach für Werbung? I: Ja, oder ... eigentlich dürften sie das ja gar nicht. A: Wieso nicht? I: Ja eigentlich steht das wohl in den Datenschutzrichtlinien drinnen, dass sie die Daten nicht nehmen von einem selbst. Müsste drinnen stehen, rechtlich gesehen, oder? A: In der Datenschutzrichtlinie? I: Ich unterschreibe ja, dass sie meine Daten verwenden dürfen, aber, dass sie ohne Erlaubnis Daten von meinem Handy verwenden können, das steht sicher in einer Datenschutzrichtlinie drinnen, dass sie das nicht dürfen. A: Aber du liest die Datenschutzrichtlinie ja nicht immer durch, woher weißt du das? I: Nein, nicht immer durch, aber das hört man immer. A: Was hört man? I: Dass sie das nicht dürfen. Einfach die Daten von deinem Handy nehmen, aber sie machen das oft trotzdem. Das merkst du ja nicht mal, wenn sie sie nehmen oder nicht. A: Kannst du das irgendwie überprüfen, ob jemand Daten von deinem Handy nimmt. Kann man das irgendwo nachschauen? I: Nein, ich wüsste das nicht. Ich wüsste nicht wo nachschauen. (Z 217-237)	Nutzen für Unternehmen: Werbung, Umsatz. eigentlich dürften sie das ja gar nicht. eigentlich steht das wohl in den Datenschutzrichtlinien drinnen, dass sie die Daten nicht nehmen von einem selbst. Müsste drinnen stehen, rechtlich gesehen, oder? Ich unterschreibe ja, dass sie meine Daten verwenden dürfen, aber, dass sie ohne Erlaubnis Daten von meinem Handy verwenden können, das steht sicher in einer Datenschutzrichtlinie drinnen, dass sie das nicht dürfen. A: Aber du liest die Datenschutzrichtlinie ja nicht immer durch, woher weißt du das? das hört man immer. aber sie machen das oft trotzdem. Das merkst du ja nicht mal, wenn sie sie nehmen oder nicht. Kannst du das überprüfen? Ich wüsste nicht wo nachschauen. (Z 217-237)	Die Person denkt sich, dass die Daten den Unternehmen nützen, um Werbung und Umsatz zu machen. Sie ist der Meinung, dass die Unternehmen nicht ohne Erlaubnis Daten von ihrem Handy verwenden dürfen, und das das in den Datenschutzrichtlinien festgehalten ist. Sie sagt, das höre man immer so, sie selbst liest die Datenschutzrichtlinien aber nicht durch. Sie ist des weiteren überzeugt, dass das die Unternehmen dennoch machen, und man selbst das gar nicht merke, ob sie Daten nehmen oder nicht. Sie weiß auch nicht wo man das überprüfen kann. (Z 217-237)	Werbung. Liest sich DSR nicht durch.

A: Was glaubst du passiert wenn eine Firma unzählig viele Daten von sehr, sehr vielen Personen speichert? I: Sie verwendet diese sicher weiter. A: Und für was? I: Ja ich denk mir Werbung, Umsatz sehen sie darin. A: Kannst du dir auch noch etwas anderes vorstellen, was man mit den Daten machen kann? I: [Schüttelt den Kopf]. (Z 238-244)	wenn eine Firma unzählig viele Daten von sehr, sehr vielen Personen speichert? Sie verwendet diese sicher weiter. ich denk mir Werbung, Umsatz sehen sie darin. Kann sich nichts anderes vorstellen, was man mit den Daten machen kann. (Z 238-244)	Der Nutzer weiß, dass Firmen mit unzählig vielen Daten Werbung und Umsatz machen können, weiß aber nicht, was man mit den Daten sonst noch machen kann. (Z 238-244)	Werbung.
Auswertungseinheit 5			
A: Was können Apps machen, die deine Fotos haben, dein Adressbuch, diese gesamten Informationen? I: Also das Adressbuch dient sicher dazu die Daten weiterzugeben, mit den Fotos fehlt mir meine Phantasie, um zu wissen, was die mit meinen Fotos anfangen könnten. (Z 223-226)	das Adressbuch dient sicher dazu die Daten weiterzugeben, mit den Fotos fehlt mir meine Phantasie, um zu wissen, was die mit meinen Fotos anfangen könnten. (Z 223-226)	Der Nutzer weiß, dass der Zugriff zum Adressbuch dazu dient, Daten weiterzugeben, bei den Fotos weiß er es nicht. (Z 223-226)	Weitergabe von Daten.
A: Wer könnte daran interessiert sein, deine Fotos zu speichern? I: Das... Ich denke Fotos haben für andere keinen Wert. Fotos haben für mich einen eigenen Wert, das ist gleich wie ich nicht die Fotos von jemand anderen haben möchte. Aber ich denke, da muss man in die Köpfe der anderen Leute rein denken. (Z 227-232)	Ich denke Fotos haben für andere keinen Wert. Aber ich denke, da muss man in die Köpfe der anderen Leute rein denken. (Z 227-232)	Der Nutzer kann sich nicht vorstellen, welchen Nutzen seine Fotos für andere haben können. Er denkt sich, dass man das verstehen kann, wenn man die Ideen anderer Leute begreift. (Z 227-232)	Kann sich Nutzen für andere nicht vorstellen.

A: Was können Unternehmen zum Beispiel machen, wenn sie nicht nur deine Daten haben, sondern von unzählig vielen Personen den Standort, die Fotos usw.? I: Das ist sicher mal eine Kontrolle, das heißt, für was sie die Kontrolle dann verwenden, das ist sicher ein (Lebens?) zum Beispiel, die Idee ist, welche einige Leute haben vom Internet her, auch vom Einkaufen her, sagt ich weiß deinen Geschmack, den sehe ich ja auf den Fotos, dann kann ich dir ja die Werbung so schicken, dass du meine Sachen kaufst. A: Also steht Verkauf und Werbung dahinter? I: Mhm. (Z 233-240)	Das ist sicher mal eine Kontrolle, ich weiß deinen Geschmack, dann kann ich dir ja die Werbung so schicken, dass du meine Sachen kaufst. steht Verkauf und Werbung dahinter? (Z 233-240)	Die Person weiß, dass mit den Daten eine Kontrolle einhergeht. Daten können auch für gezielte Werbung und Verkauf benutzt werden. (Z 233-240)	Kontrolle. Gezielte Werbung. Verkauf.
A: Ok. Welche Folgen kann das für uns noch haben? I: Es ist sicher auch im Gesetz, abgesehen davon, dass Datendiebstahl gesetzlich nicht erlaubt ist, aber ich denke mir einfach mal weiß einfach nicht was in den Köpfen der Leute vorgeht. Wenn jemand beginnt jemanden nachzuspionieren aus irgendeinem Grund, dann ist das nicht angenehm, wenn er meine Fotos hat und mir dann diese Fotos womöglich mit der Post schickt. (Z 241-246)	Datendiebstahl gesetzlich nicht erlaubt ist. Wenn jemand nachspioniert, dann ist das nicht angenehm, wenn er meine Fotos hat. (Z 241-246)	Der Nutzer verbindet Datenspeicherung mit Datendiebstahl. Folgen: Nicht angenehm, wenn andere Daten von uns haben. (Z 241-246)	Unangenehm. Überwachung. Datendiebstahl.
Auswertungseinheit 6			
A: Mhm. Was nutzt ihnen das, wenn sie wissen, wer zu wem gehört und wie das zusammengestellt ist? I: Hm. Bo, ich glaube ich hab mal gehört, dass man diese Daten auch verkaufen kann, dass man da auch so Handel machen kann. Ich weiß nicht, dann bekommst auch Werbungen zugeschickt, von diesen Sachen. A: Ja, wo hast du davon gehört? Weißt du das noch? In Nachrichten oder von anderen Leuten? I: Keine Ahnung, Allgemeinwissen, nein. (lacht). (Z 187-194)	Was nutzt ihnen das? ich hab mal gehört, dass man diese Daten auch verkaufen kann, dass man da auch so Handel machen kann. Ich weiß nicht, dann bekommst auch Werbungen zugeschickt, von diesen Sachen. (Z 187-194)	Glaubt mal gehört zu haben, dass Daten verkauft werden können und dass man genaue Werbung zugeschickt bekommt. (Z 187-194)	Werbung.

A: Ja, und mit diesen Daten macht er dann wieder das gleiche? I: Sich alles zusammenstellen, ja. A: Gut, wieso werden diese Daten gespeichert? I: Damit man alles zurückverfolgen kann. A: Mhm. Kontrolle? I: Ja. Bo, sonst geht es vielleicht auch um die Sicherheit. A: Für dich selbst jetzt oder für andere Leute vielleicht, oder für beides? I: Bo, allgemein eigentlich. Für andere Leute auch zum Beispiel. Es gibt ja nicht ganz ehrliche Leute, dass keine Ahnung, die Polizei da ein bisschen schauen kann. (Z 217-225)	Sich alles zusammenstellen, ja. I: Damit man alles zurückverfolgen kann. Kontrolle? vielleicht auch Sicherheit allgemein . Es gibt ja nicht ganz ehrliche Leute, dass keine Ahnung, die Polizei da ein bisschen schauen kann. (Z 217-225)	Die Person weiß, dass die App Daten von nicht funktionsgebundenen Bereichen braucht, um sich ein Netz an Daten über uns zu verschaffen und somit Handlungen zurückverfolgen zu können. Sie denkt, dass es nicht unbedingt nur zur Kontrolle, sondern auch zur Sicherheit von allen, allgemein beitragen kann, weil nicht alle Menschen nur Gutes tun und es der Polizei somit erleichtert wird. (Z 217-225)	Überblick.
I: Nein, keine Ahnung. Bei Dings-Da weiß ich halt, wenn du verschiedene Sachen eingibst bei Google oder Facebook, dann kommen genau diese Werbungen, wofür du dich interessiert hast. A: Ok, dass sie sich dann genau ansprechen können? I: Ja, ganz genau. (Z 239-243)	dann kommen genau diese Werbungen, wofür du dich interessiert hast. A: Ok, dass sie sich dann genau ansprechen können? I: Ja, ganz genau. (Z 239-243)	Die Person weiß, dass ihre Daten dazu verwendet werden, ihr gezielte Werbung zu schicken, welche sie ansprechen sollte. (Z 239-243)	Personalisierte Werbung.
A: Was kann das für uns welche Folgen haben, wenn über uns alle Daten offen sind? I: Keine Ahnung. Ich weiß nicht, was da welche Nachteile sind. (Z 244-245)	Was kann das für uns welche Folgen haben, wenn über uns alle Daten offen sind? I: Keine Ahnung. Ich weiß nicht, was da welche Nachteile sind. (Z 244-245)	Die Person weiß nicht, welche Folgen das für uns haben kann, wenn unsere Daten für alle zugänglich sind. (Z 244-245)	Weiß nicht welche Nachteile möglich sind.
A: Aber könntest du dir vorstellen, dass wenn du rausfindest, dieser Dienst nimmt sehr viele Daten von mir, dass du diesen dann beendest, weil du sagst, das möchte ich nicht? I: Eigentlich, ich weiß jetzt nicht, welchen Nachteil das hat, wenn jemand die Daten hat über einen anderen. (Z 251-254)	Eigentlich, ich weiß nicht, welchen Nachteil das hat, wenn jemand die Daten hat über einen anderen. (Z 251-254)	Auch wenn die Person rausfinden würde, dass eine App sehr viele Daten von ihr speichert, weiß sie nicht was sie machen würde, weil sie nicht weiß, welchen Nachteil die Datenspeicherung für sie hat! (Z	Weiß nicht welche Nachteile möglich sind.

		251-254)	
Auswertungseinheit 7			
A: Was können Unternehmen machen, wenn sie unzählig viele Daten von unzählig vielen Leuten besitzen? Was ist da der Gedanke dahinter? I: Werbezwecke? Würde ich jetzt so spontan sagen. Nein ich weiß es nicht. A: Sonst noch irgendwas? Was sie mit den Daten alles machen können? Oder wie benützen sie diese Daten für die Werbung? I: Ja keine Ahnung, entweder da sind E-Mails drauf, dann kannst du E-Mail-Werbung machen, oder sonst Telefonnummern, das weiß ich jetzt nicht. Oder sie verkaufen die Kontakte, das könnte auch sein. A: Wer oder wieso könnte da überhaupt jemand interessiert sein die Kontakte zu kaufen? I: Ja zum Werben. Immer!(Z278-287)	Werbzwecke? Würde ich spontan sagen. E-Mail-Werbung, oder Telefonnummern, das weiß ich jetzt nicht. Oder sie verkaufen die Kontakte. Interessiert immer zum Werben. (Z 199-214)	Die Person weiß nicht genau, was es einem Unternehmen nützt viele Daten zu besitzen. Sie vermutet für Werbezwecke, immer, oder um Kontakte zu verkaufen, wobei immer Werbung der Gedanke bleibt. (Z 199-214)	Werbung. Weiß keine Alternativen.

Auswertungseinheit 8			
A: Wenn du dir jetzt vorstellst, eine App hat unzählig viele Daten, nicht nur von dir, sondern von ganz, ganz vielen Leuten. Was könnten dann die Folgen für uns sein, wenn diese alles über uns wissen, also nicht nur über uns zwei, sondern über uns alle. I: Erpressung, Ausnutzung. So irgendwas. A: Mhm. Und wie könnten sie das machen? Wie machen sie diese Erpressung oder Ausnutzung? Wie würde das funktionieren? I: Mit, keine Ahnung, Verträge oder irgendwas, dass sie sagen, schau ich habe das und das von dir. Du musst das und das. Vor allem bei den Bankdaten muss man sich sehr aufpassen meiner Meinung nach. Da können sie ja auch das ausnutzen und dir irgendeine Klausel dreingeben, wo du sagst, da habe ich gar nie zugestimmt, aber im Grunde hast du es nie durchgelesen. A: Meinst du jetzt auch Kreditkarten, wenn du diese angibst, dass sie dir dann immer was abbuchen, was du aber eigentlich gar nicht möchtest. I: Genau. Es heißt zwar immer, es sei gratis die Nutzung zum Beispiel, aber dann musst du alles angeben. Und es heißt zwar, es werde nicht belasten, aber dann im Kleingedruckten steht wieder was anderes und solche Sachen. Ja. (Z 199-214)	Erpressung, Ausnutzung. Wie würde das funktionieren? Keine Ahnung, Verträge. Es heißt zwar immer, es sei gratis die Nutzung zum Beispiel, aber dann musst du alles angeben. Und es heißt zwar, es werde nicht belasten, aber dann im Kleingedruckten steht wieder was anderes und solche Sachen. (Z 199-214)	Folgen für uns, wenn ein Unternehmen sehr viele Daten über uns hat: - Erpressung - Ausnutzung - Bei Verträgen, wo man Kreditkarten oder Bankdaten eingibt, aufpassen. - Kleingedrucktes lesen, was man unterschreibt. (Z 199-214)	Erpressung. Ausnutzung.
A: Das heißt wie werden die Daten von der App dann weiterverarbeiten, wenn sie Zugriff haben auf dein Handy. I: Da bin ich jetzt überfragt. (Z215-217)	Da bin ich überfragt. (Z215-217)	Überfragt, wie Daten weiterverarbeitet werden. (Z215-217)	Weiß nicht wie weiterverarbeitet.

Auswertungseinheit 9			
A: Welchen Grund haben die Geheimdienste Daten zu speichern überhaupt? I: Keine Ahnung, wenn jemanden das nicht bewusst ist, dass die darauf Zugriff haben, dann könnte man ja, ganz krass gesagt, über Facebook was planen und aushacken. Dass sie dahinter kommen. A: Praktisch Kontrolle? I: Ja. (Z 187-192)	Wenn jemand nicht bewusst ist, dass sie darauf Zugriff haben, dann könnte man ja über Facebook was planen. Dass sie dahinter kommen. Kontrolle. (Z 187-192)	Die Person weiß, dass wenn kriminelle Handlungen online geplant werden, dass betreffende Person kontrolliert werden. (Z 187-192)	Kontrolle/Überprüfung.
A: Was meinst du können jetzt Geheimdienste wie die NSA, aber auch andere Unternehmen, die ganz viele Daten haben, sagen wir mal eine Firma von einer App, die unzählig viele Daten von ganz, ganz vielen Leuten haben. Was können sie mit diesen Daten anfangen? Welchen Vorteil bringen ihnen diese vielen Daten? I: Überprüfung. A: Von was? I: Wie viele registriert sind. Wo vielleicht. Wo auf der Welt, dass mehr registriert sind. Altersgruppen. A: Können sie dann irgendwas daraus schließen? I: Ja, eigentlich schon. Keine Ahnung, wenn es nur junge Leute nehmen, dann wird es für ältere wohl zu kompliziert sein oder weißt du, so Schlussfolgerungen halt von den vielen Daten. A: Dass sie das dann an jemanden anpassen können? I: Ganz genau. (Z 193-206)	Überprüfung, wie viele registriert sind, wo, Altersgruppen. Schlussfolgerungen von den vielen Daten. An Personen anpassen. (Z 193-206)	Die Person weiß, dass die Daten den Unternehmen Aufschluss geben, wie viele Nutzer, wo registriert sind und sie daraus das Angebot optimieren können. (Z 193-206)	

A: Das sind im Grunde die Vorteile auf der einen Seite für das Unternehmen. Kann das für uns auch vor oder Nachteile haben? I: Ja, keine Ahnung, dass die App angepasst wird, vielleicht. A: Ja, das ist ein Vorteil für uns. Gibt es auch Nachteile? I: Ja, die haben halt immer die Daten von dir. A: Das heißt du kannst überprüft werden? I: Ja. Genau. Also die Privatsphäre ist dahin. Also auf ein Minimum reduziert. (Z 207-213)	Gibt es auch Nachteile? Die haben halt immer die Daten von dir. Also die Privatsphäre ist dahin, auf ein Minimum reduziert. (Z 207-213)	Die Vorteile für den Nutzer sind die Anpassung der App an die jeweiligen Bedürfnisse, die Nachteile, dass das Unternehmen alle Daten über einen selbst hat, eine Überprüfung erleichtert wird und die Privatsphäre auf ein Minimum reduziert ist. (Z 207-213)	Weniger Privatsphäre. Unangenehm. Überwachung.
Auswertungseinheit 10			
A: Du hast gesagt diese Apps nutzten deine Daten für Werbung. I: Ja. A: Kannst du dir ein anderes Ziel außer Werbung noch vorstellen? Dass es da noch ein anderes Ziel gibt, dass es praktisch nicht nur die Werbung gibt, die interessant ist für sie? I: Naja, für den Staat, wie man jetzt bei den NSA herausgefunden hat ist Spionage auch interessant. Wie man da gehört hat, haben sie da auch auf die Google-Server zugegriffen. (Z 188-193)	Naja, für den Staat, wie man jetzt bei den NSA herausgefunden hat ist Spionage auch interessant. Wie man da gehört hat, haben sie da auch auf die Google-Server zugegriffen. (Z 188-193)	Der Nutzer spricht die Verwendung der Daten für Spionage und aktuelle Geschehnisse an. (Z 188-193)	Erklärung des Zusammenhangs. Aktuelle Geschehnisse. Spionage. (Z 188-193)
A: Was wollen sie im Grunde mit Spionage erreichen? I: Ja, das eine ist Wirtschaftsspionage, nicht direkt aber halt so, und das andere ist die aktive Kontrolle von der Masse. Wenn du die Masse kontrollieren kannst, beziehungsweise ihre Gedanken nachvollziehen, hast du als Staat mehr Macht und mehr Kontrolle über dein eigenes Volk. (Z 194-198)	das eine ist Wirtschaftsspionage, nicht direkt aber halt so, und das andere ist die aktive Kontrolle von der Masse. Wenn du die Masse kontrollieren kannst, beziehungsweise ihre Gedanken nachvollziehen, hast du als Staat mehr Macht und mehr Kontrolle über dein eigenes Volk. (Z 194-198)	Der Nutzer erklärt, welchen Nutzen die Spionage haben kann und in welchem Bereich. Macht und Kontrolle durch den Staat. (Z 194-198)	Macht. Kontrolle.

A: Was meinst du können Unternehmen machen, wenn sie unzählig viele Daten von unzählig vielen Leuten besitzen? Was meinst du machen diese mit denen? I: Ja zuerst mal in Datenbanken einspeichern, Datenbanken vergleichen und durch irgendwelche komplizierte Programme durchlaufen lassen, die Programme dann noch filtrieren, was du so suchst. Und dir dann automatisch wieder – ihnen Information mehr oder weniger was diese Person, natürlich macht das alles ein Computer, weil für einen Menschen wäre das zu viel. A: Das heißt die werden gut verarbeiten und analysiert? I: Ja, sie werden analysiert und verarbeiten, ich meine natürlich wird von Person XY, werden jetzt nicht Mitarbeiter, Bilder zu sehen bekommen. Sie können es, wenn sie wollen, aber ich glaube nicht, dass mein Bild irgendjemand, keine Ahnung, der in Kalifornien in einer Zentrale arbeitet, alle meine Bilder sieht. Natürlich können sie es, wenn sie wollen, aber ich sage, das wird automatisch verarbeiten. (Z 199-211)	in Datenbanken einspeichern, Datenbanken vergleichen und durch komplizierte Programme durchlaufen lassen, die Programme dann noch filtrieren, was du so suchst. Und dir dann automatisch wieder – ihnen Information mehr oder weniger was diese Person, natürlich macht das alles ein Computer, weil für einen Menschen wäre das zu viel. Sie werden analysiert und verarbeiten, ich meine natürlich wird von Person XY, werden jetzt nicht Mitarbeiter, Bilder zu sehen bekommen. Sie können es, wenn sie wollen, aber ich glaube nicht, dass mein Bild irgendjemand, keine Ahnung, der in Kalifornien in einer Zentrale arbeitet, alle meine Bilder sieht. Natürlich können sie es, wenn sie wollen, aber ich sage, das wird automatisch verarbeiten. (Z 199-211)	Der Nutzer weiß, wie die Datenanalyse und -Speicherung zusammenhängen und kann sehr genau die einzelnen Prozesse erklären. Er spricht die automatische Verarbeitung an. (Z 199-211)	Sehr detaillierte Erklärung.
--	--	---	-------------------------------------

Auswertungseinheit 11			
A: Was können sie machen mit diesen Adressen? I: Werbungen schicken, verkaufen. Ich denke das ist der Hauptgrund. A: Meinst du gibt es noch einen Grund, dass Firmen das machen, außer Werbung? I: Daten sind immer beliebt. Also ich denke unabhängig, ob das alles brauchbare Daten sind, je mehr du hast, hast du halt viele. A: Was kannst du mit diesen Daten machen, wenn du viele hast? I: Gut, du kannst sie verkaufen, du kannst sie auch nur benutzen um selbst Sachen auszuschieken, um selbst Werbung zu machen wahrscheinlich. Du kannst mit diesen Daten viel anfangen, glaube ich. A: Vor allem im Werbebereich jetzt? I: Immer im Werbebereich, weil sonst bringt dir das ja nichts eigentlich. Ich glaube das ist alles nur für den Werbebereich geeignet, dass du die Daten besitzt. Gleich ist es bei Firma 3, wenn du viele Daten hast, umso mehr Newsletter kannst du rausschicken. Je mehr Daten du hast, umso mehr Personen erreichst du. Das wird da das gleiche sein. (Z 180-193)	Werbung schicken, verkaufen. Das ist der Hauptgrund. Daten sind immer beliebt, du kannst sie verkaufen, Werbung machen. Immer im Werbebereich, nur für den Werbebereich geeignet. Je mehr Daten du hast, umso mehr Personen erreichst du. (Z 180-193)	Der Nutzer weiß, dass die Daten den Unternehmen hauptsächlich für Werbung dienen. Je mehr Daten man hat, umso mehr Menschen kann man erreichen. Daten für Sonstiges nicht geeignet. (Z 180-193)	Werbung.

A: Was meinst du, wenn jetzt ein Unternehmen nicht nur von dir viele Daten besitzt, sondern auch unzählig viele Daten von unzählig vielen anderen Leuten in verschiedenen Bereichen? Was nutzt das diesem Unternehmen? I: Macht, denke ich auch. Ich meine, wenn du weißt, ich habe jetzt von Millionen von Leuten die Daten, ist das sicher auch etwas was in der Konkurrenz auch mit Macht zu tun hat. Auch mit Vorsprung, wenn du mehr Daten hast, wie andere. Ob das jetzt wirklich was bringt, weiß ich auch nicht, aber ich denke schon. Also kann nicht schlecht sein, kann ja nur gut sein. (Z 194-200)	Macht, denke ich auch. Ich meine, wenn du weißt, ich habe jetzt von Millionen von Leuten die Daten, ist das sicher auch etwas was in der Konkurrenz auch mit Macht zu tun hat. Auch mit Vorsprung, wenn du mehr Daten hast, wie andere. Ob das jetzt wirklich was bringt, weiß ich auch nicht, aber ich denke schon. Also kann nicht schlecht sein, kann ja nur gut sein. (Z 194-200)	Die Person ist überzeugt, dass Daten Macht bringen. (Z 194-200)	Macht.
A: Macht ist sicher ein Punkt, aber die Macht muss ich ja ausnutzen, ich muss mit den Daten ja auch irgendwas machen, damit es zur Macht wird. Hast du eine Vorstellung wie aus Daten Macht wird? I: Kaufen, verkaufen, Werbung. A: Und was machen diese Unternehmen, die Daten kaufen? Werbung schicken, denke ich mir mal. (Z 201-206)	Die Macht entsteht durch das kaufen, verkaufen von Daten und durch Werbung. (Z 201-206)	Die Person weiß, dass man die Daten kaufen, verkaufen kann und Werbung einsetzen muss, damit Daten zur Macht werden. (Z 201-206)	Werbung. Macht.

A: Und, wenn diese Daten jetzt analysiert werden, weil das müssen sie ja, wenn du eine Werbung erstellen willst, ist es dann möglich, dass man bei der Auswertung schon Besonderheiten aus den Daten sehen kann? I: Das hängt davon ab, wenn du jetzt nur die Daten hast von einem Benutzer, der die App benutzt, kannst du sicher eine gute Statistik machen. Aber wenn du jetzt wirklich alle Adressen hernimmst, dann weißt du ja nicht wer was benützt. Also ich denke, wenn du jetzt die Daten hernimmst von dem Benutzer, der die App benutzt, ist das sicher super, um Statistiken zu erstellen, wo du auch sehen kannst wie viel Prozent der Nutzer zum Beispiel männlich sind, wie viele weiblich, zum Beispiel. Aber wenn du jetzt wirklich alle Daten vom Adressbuch nimmst, weiß ich nicht wie viel du damit erreichen kannst. Weil da hast du ja nur die Daten, du weißt ja nicht, was diese verschiedenen Kontakte machen. Du weißt ja nur den Kontakt. (Z 216-227)	Das hängt davon ab, wenn du jetzt nur die Daten hast von einem Benutzer, der die App benutzt, kannst du sicher eine gute Statistik machen. Aber wenn du jetzt wirklich alle Adressen hernimmst, dann weißt du ja nicht wer was benützt. Also ich denke, wenn du jetzt die Daten hernimmst von dem Benutzer, der die App benutzt, ist das sicher super, um Statistiken zu erstellen, wo du auch sehen kannst wie viel Prozent der Nutzer zum Beispiel männlich sind, wie viele weiblich, zum Beispiel. Aber wenn du jetzt wirklich alle Daten vom Adressbuch nimmst, weiß ich nicht wie viel du damit erreichen kannst. Weil da hast du ja nur die Daten, du weißt ja nicht, was diese verschiedenen Kontakte machen. Du weißt ja nur den Kontakt. (Z 216-227)	Die Person denkt, dass nur die Analyse von einem Nutzer aufschlussreiche Statistiken hervorbringt. Sie kann sich den Nutzen von bloßen Zusammenhängen nicht als wertschöpfend vorstellen. Die Person versteht den größeren Gedanken von Big Data nicht. Sie denkt, sobald man mehr Daten hat und diese nicht mehr zuordnen kann, verlieren die Daten an Wert. (Z 216-227)	Statistik. Versteht den Zusammenhang nicht.
A: Kannst du dir aber vorstellen, dass man das schon so genau zusammensuchen kann, dass man sogar sagen kann wer mit wem und wie und was zu tun hat? I: Ah ja, sicher. Ich glaube, das sieht man auch bei Facebook. Wenn du reingehst, dass du siehst wer mit wem befreundet ist, was derjenige macht usw. (Z 228-231)	Ah ja, sicher. Ich glaube, das sieht man auch bei Facebook. Wenn du reingehst, dass du siehst wer mit wem befreundet ist, was derjenige macht usw. (Z 228-231)	Person glaubt aber dann wieder, dass man herausfinden kann, wer mit wem in Verbindung steht und was sie machen. Beispiel Facebook. (Z 228-231)	Uneinigkeit.

Abstract - deutsch

Big Data verkörpert die Möglichkeit aus vielen, scheinbar unnützen Daten wertvolle Informationen zu schöpfen. Diese Möglichkeit birgt aber auch viele Gefahren, weshalb ein bewusster Umgang mit unseren Daten unerlässlich ist. Die Literatur im Bereich der Big Data – Debatte setzt sich vor allem mit den Möglichkeiten und Folgen von Big Data auseinander. Da jedoch Studien, wie jene von Yong Jin Park et al. belegen, dass das Wissen eine große Rolle beim Online-Datenschutz spielt und Wissen signifikant mit einem besseren Schutz der Daten, sei es in sozialer, als auch in technischer Dimension, einhergeht,⁴⁰⁵ wird mit dieser Studie angestrebt, die Frage über den Wissensstand der Smartphonebenutzer zu beantworten. Als Untersuchungsteilnehmer wurden 18- bis 24-jährige Konsumenten gewählt, da laut einer DIVISI-Studie besonders junge Menschen das Smartphone intensiv nutzen und sehr häufig über das Smartphone das Internet verwenden.⁴⁰⁶

In dieser Arbeit wird hinterfragt, was junge Erwachsene überhaupt über Big Data und seine Möglichkeiten, wie auch Risiken, wissen. Mit Hilfe der qualitativen Methode der persönlich geführten Leitfadeninterviews und der anschließenden qualitativen Inhaltsanalyse konnte ein mangelndes Wissen im Hinblick auf Big Data, seine Risiken und Folgen festgestellt werden.

Ein Ungleichgewicht herrscht dabei bei dem Faktenwissen und dem Strukturwissen. Besonders das Bewusstsein für den Schutz der eigenen Daten während der Benutzung des Smartphones mit all seinen Funktionen muss gestärkt werden, um einen ausreichenden Schutz vor den möglichen Folgen einer Big Data – Zukunft zu sichern.

Diese Studie soll daher einerseits als Anregung für weiterführende Studien in diesem Bereich der Kommunikationswissenschaft dienen, andererseits aber auch Anlass zu einer breiten medialen Aufmerksamkeit geben.

⁴⁰⁵ Vgl. Yong Jin Park et al, 2012. S. 1024

Abrufbar unter: <http://www.sciencedirect.com/science/article/pii/S0747563212000064> (03.07.2014).

⁴⁰⁶ Vgl. DIVISI U-25-Studie, 2014. S. 65

Abstract - english

Big Data refers to the possibility of obtaining useful information from a lot of apparently useless data people leave on the internet wherever they go. As this includes also big risks, the awareness of users when dealing with personal data is essential. Existing literature mainly focuses on the possibilities and risks associated with Big Data. But studies, like Yong Jin Park et al. show, that there is an interplay between the knowledge of data protection and the privacy protective behaviour. They suggest that the amount of knowledge regarding data collection risk and regulatory protection significantly predicts a higher level of social and technical privacy protection.⁴⁰⁷ Based on these results, this thesis focuses on what young adults know about big data, including its possibilities and risks. Therefore a semi-structured interview with 18–24 year old smartphone users about their knowledge of big data was conducted. The focus on this group is based on a DIVISI-research that suggests that adults between 18- and 24 years use their smartphones frequently for getting access to the internet.⁴⁰⁸ Qualitative content analysis showed that the amount of knowledge of young adults is insufficient for an adequate level of data protection. More specifically, this study was able to find an imbalance between factual and structural knowledge of the users. Especially the awareness for data protection while the usage of the applications of the smartphone should to be enhanced for a sufficient protection from bad consequences of a possible Big Data future. Due to the importance of big data as well as the results of this master thesis further research on this topic related to communications and increased media awareness is strongly recommended.

⁴⁰⁷ Vgl. Yong Jin Park et al, 2012. S. 1024

⁴⁰⁸ Vgl. DIVISI U-25-Studie, 2014. S. 65

Curriculum Vitae

Barbara Mayr, Bakk. phil. BA

Bildungsweg:

Seit Oktober 2012	Magisterstudium Publizistik- und Kommunikationswissenschaft an der Universität Wien
10/2008 – 07/20012	Bakkalaureatstudium Publizistik- und Kommunikationswissenschaft an der Universität Wien
07/2008	Matura am Realgymnasium Bruneck
09/2000 – 07/2003	Mittelschule Dr. Josef Röd Bruneck
09/1995 – 06/2000	Volksschule Reischach

Berufserfahrung:

Seit 02/2014	Selbständige Tätigkeit als Coach im Bereich Business und Fitness
08/2012 – 09/2012	Südtiroler Tageszeitung Dolomiten, Lokalseite Pustertal <i>Pressepraktikum</i>
06/2012	Wochenmagazin FF <i>Pressepraktikum</i>
07/2011 – 08/2011	Sonntagszeitung Zett <i>Pressepraktikum</i>
09/2010	PR-Agentur Succus <i>PR-Praktikum</i>

Sprachkenntnisse:

Deutsch	Muttersprache
Italienisch	Zweitsprache, fließend
Englisch	sehr gut