HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELOR ARBEIT

Frau
Sarah Schmidbauer

Beeinflusst die staatliche Überwachung der Social-Media-Kommunikation das Verhalten junger Nutzer?

2017

Fakultät: Medien

BACHELOR ARBEIT

Beeinflusst die staatliche Überwachung der Social-Media-Kommunikation das Verhalten junger Nutzer?

Autor/in:
Frau Sarah Schmidbauer

Studiengang:
PR- und Kommunikationsmanagement

Seminargruppe:
AM15sK1-B

Erstprüfer:
Rechtsanwalt **Professor Markus Heinker, LL.M.**

Zweitprüfer:
Professor Doktor Rudolf Dolzer

Einreichung: 8.1.2018

Faculty of Media

BACHELOR THESIS

Does the state monitoring of the communication in social media changes the behaviour of young users?

author:
Ms. Sarah Schmidbauer

course of studies:
Public Relation and Communicationmanagement

seminar group:
AM15sK1-B

first examiner:
Rechtsanwalt **Professor Markus Heinker, LL.M.**

second examiner:
Professor Doctor Rudolf Dolzer

submission:
8.1.2018

Bibliografische Angaben

Nachname, Vorname: Schmidbauer, Sarah

Thema der Bachelorarbeit: Beeinflusst die staatliche Überwachung der Social-Media-Kommunikation das Verhalten junger Nutzer?

Topic of thesis: Does the state monitoring of the communication in social media changes the behaviour of young users?

55 Seiten, Hochschule Mittweida, University of Applied Sciences,
Fakultät Medien, Bachelorarbeit, 2017

Abstract

Die staatliche Überwachung ist ein ständiger Begleiter in unserem Alltag. In dieser Bachelor Arbeit soll Einblick in die Welt der digitalen Kommunikation und der staatlichen Überwachung geboten werden. Die explorative Studie soll aufzeigen, welche sozialen und rechtspolitischen Folgen die staatliche Überwachung mit sich bringt und Überlegungen dazu gestatten, ob sich für den Gesetzgeber neue Aufgaben ergeben.

Inhalt

Abkürzungsverzeichnis

NSA	National Security Agency
CIA	Central Intelligence Agency
BND	Bundesnachrichtendienst
BfV	Bundesamt für Verfassungsschutz
etc.	et cetera, et cetera

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Alle Menschen auf dieser Welt sind in irgendeiner Weise auf digitaler Ebene miteinander verbunden. Heutzutage kann jeder über die sozialen Netzwerke kommunizieren. 2013 dann das große Erwachen. Whistleblower Edward Snowden - ein ehemaliger Mitarbeiter der National Security Agency - veröffentlichte streng geheime Daten seiner ehemaligen Arbeitsstelle. Damals kam zum Vorschein, wer durch die NSA überwacht wird. Doch auch Unternehmen, die anscheinend mit den Geheimdiensten zusammen gearbeitet haben, werden in den Unterlagen genannt.

Staatliche Überwachung bedeutet, dass ein Staat seine Bürger mit einer Vielzahl staatlich legalisierter technischer Mittel überwacht. Der Begriff ist in vielen Teilen der Bevölkerung negativ besetzt und bedeutet, dass die Überwachung ein zentrales Merkmal des staatlichen Handelns geworden ist. Hier stellt sich die Frage: Verändern die Menschen aufgrund der Überwachung ihr allgemeines Verhalten? Was hat der Chilling Effect damit zu tun? Wer überwacht überhaupt wen? Wie lassen sich die Grundrechte mit der Überwachung vereinbaren?

Die Forschungsfrage beschäftigt sich mit der Zukunft. Doch Vergangenheit und Gegenwart können entscheidend dafür sein, wie die Zukunft aussehen könnte. Ziel der Arbeit soll sein, heraus zu finden, ob staatliche Überwachung einen Einfluss auf die Social-Media-Kommunikation der jungen Nutzer hat und haben wird.

1.1. Hinführung zur Thematik

In der Bachelor Arbeit wird es darum gehen, was das Informationelle Selbstbestimmungsrecht mit der staatlichen Überwachung zu tun hat, welche staatlichen Überwachungsorganisationen es gibt, deren Geschichte und was normale Unternehmen damit zu tun haben. Des Weiteren werden die Geschichten von WhatsApp und Facebook dargestellt und sowohl Online-Kommunikation als auch die Möglichkeiten für Datenschutz erläutert. Es folgt eine Pro und Contra Aufstellung zu Überwachung versus Freiheit. Außerdem werden mögliche Folgen der totalen Überwachung aufgezeigt.

Nach der Literaturanalyse erfolgt die empirische Untersuchung der Forschungsfrage anhand von Interviews durch Experten und Passanten. Anschließend werden diese Ergebnisse ausgewertet und verglichen. Diese Forschung ist rein explorativ und somit nicht repräsentativ. Diese Untersuchung soll Aufschluss über das zukünftige Verhalten der Nutzer in Bezug auf die Social-Media-Kommunikation liefern.

Das Thema „Beeinflusst die staatliche Überwachung der Social-Media-Kommunikation das Verhalten junger Nutzer“ ist sowohl Alt als auch Neu. Alt, da es sehr viele Veröffentlichungen und Ergebnisse über Verhaltensänderungen gibt. Neu, da die Zukunftsprognose nicht über 2016 reicht. Dies wird Ziel der Arbeit sein. Es soll ermittelt werden, ob die staatliche Überwachung das Verhalten junger Nutzer tatsächlich verändert und wenn ja, wie sehr das geschieht.

Diese Arbeit befasst sich nicht mit der Frage, welche Konsequenzen der Staat aus dem möglichen Ergebnis einer Befragung ziehen sollte. Dies wäre eine eigene Untersuchung Wert. Hier soll lediglich darauf hingewiesen werden, dass eine dauerhaft negative Einstellung der Bevölkerung zur Überwachung in sich selbst den Fortbestand der bestehenden Überwachung in Frage stellen könnte.

2. Gegenstand der explorativen Studie

Im Lichte der noch zu erörternden Formen der Kommunikation und ihrer immer weiteren Ausbreitung soll sich die explorative Studie mit der Überwachung dieser Arten der Kommunikation durch den Staat befassen. Eine der wichtigsten Aufgaben eines jeden Staates ist es, die Sicherheit seiner Bürger zu schützen. Die explorative Studie soll aufzeigen, welche sozialen und rechtspolitischen Folgen die staatliche Überwachung mit sich bringt und Überlegungen dazu gestatten, ob sich für den Gesetzgeber neue Aufgaben ergeben. Die Studie geht nur auf die Überwachung durch den Staat ein. Dabei wird nicht übersehen, dass die neuen Formen der Kommunikation auch insoweit Probleme aufwerfen, als eine Überwachung technisch auch durch private Unternehmen oder auch einzelne Staatsbürger möglich erscheinen; in mancher Hinsicht mag die Überwachung von Privaten durch Private ebenso bedeutsam sein, wie die Überwachung durch den Staat. Die enorme Größe von Google etwa und seine gigantischen technischen Kapazitäten weißen auf die Probleme durch die privaten Formen der Überwachung hin.

Dennoch beschränkt sich die hier untersuchte Studie auf die staatliche Überwachung und die damit verbundenen Fragestellungen und Probleme; dies ist dadurch gerechtfertigt, das sich bei der Überwachung durch Private andere Probleme ergeben, die getrennt zu untersuchen wären. Von Bedeutung ist bei der Festlegung der Studie, auf welchen Informations- oder Handlungsbedarf der Gegenstand zugeschnitten sein soll. Von Interesse wäre diese etwa für die Medien und die Öffentlichkeit im Allgemeinen. Hier wird davon ausgegangen, das insbesondere der Bundestag im Hinblick auf seine Aufgaben für die staatliche Überwachung der Information über die Einstellung der Bevölkerung zu diesem Themenkreis bedarf. Letztlich wird die Studie aber so verstanden, dass sie auch für die Medien und die Öffentlichkeit sinnvolle Aussagen über die künftigen Arten der Überwachung erlauben soll.

3. Social-Media-Kommunikation

Zu Beginn dieser Arbeit sollen zunächst einige Punkte verdeutlicht werden. Unter anderem, wie sich die Social-Media-Kommunikation entwickelt hat und was Online-Kommunikation bedeutet. Im Anschluss sollen die Entstehung von Facebook und WhatsApp deutlich machen, wie sehr soziale Netzwerke in den Vordergrund gerückt sind und warum Facebook und WhatsApp als Basis der Forschungsarbeit fungieren.

3.1. Die Entwicklung der Social-Media-Kommunikation

Facebook, WhatsApp und ICQ. Sie alle haben das Leben von vielen Menschen dermaßen verändert, dass sie erst bei einem Komplettausfall realisieren würden, wie groß diese Veränderung ist. Heute gehören Social-Media-Kanäle so zu unserem Alltag, dass man meinen könnte, es würde sie schon immer geben. Im Folgenden wird die Geschichte der sozialen Netzwerke genauer unter die Lupe genommen. Für die Arbeit ist es insofern wichtig, als dass aufgezeigt werden soll, wie sehr Facebook und Co. unser Leben verändert hat.

Der Grundstein für eine neue Kommunikationsart wurde 1970 gelegt. Damals wurde die erste E-Mail von Roy Tomlinson versendet. Auch das @-Zeichen stammt von ihm. Somit war diese Mail der Start für das Internet und die digitale Kommunikation.[1] Ebenfalls 1971 wurde das Usenet online gestellt. Dies war ein Forum, das Nutzern die Möglichkeit gab, über bestimmte Themenbereiche zu diskutieren. Wichtig ist hierbei zu erwähnen, dass das Internet somit aus dem Wunsch nach Kommunikation und Austausch entstand.

Nachdem 1989 das „World Wide Web“ entwickelt wurde, hat der Student Justin Hall fünf Jahre später den ersten Blog veröffentlicht. Sein Ziel war es, sich durch den Blog mit anderen Menschen zu verbinden und untereinander zu kommunizieren. Kurz darauf wurde der Grundstein für die erste Social Media Seite gelegt. Auf „Classmate“ konnte man ehemalige Schulkameraden finden und somit kommunizieren und sein soziales Netzwerk vergrößern. Man konnte sich also nicht real sondern virtuell vernetzen.[2] Die erste Suchmaschine - und somit der Vorgänger von Google war ask.com, welche ebenfalls 1994 entstanden ist.

Das Jahr 2000 war das Zeitalter der Sozialen Netzwerke. Diese bedeuten, dass die Nutzer dieser Plattformen Inhalte hochladen und teilen können. So entstand im Januar 2000 „friendster“ und „myspace“. Ebenfalls im Januar wurde das große Wikipedia gegründet. Ziel war es, genau wie das der sozialen Netzwerke, Inhalte gemeinschaftlich

[1] http://www.kundengewinnung-im-internet.com/social-media-geschichte/
[2] http://www.kundengewinnung-im-internet.com/social-media-geschichte/

zu veröffentlichen. Jimmy Wales und Larry Sanger (die Gründer von Wikipedia) schufen somit ein open-source Wissensportal, das von den Nutzern mit gestaltet werden konnte.

2004 kam Facebook auf den Markt. Dieses Netzwerk veränderte alles vorherige und setzte einen neuen Maßstab. Mark Zuckerberg gründete Facebook, um für Harvard Studenten ein Netzwerk zu schaffen. Dass das Netzwerk am Ende so groß werden würde, war nicht die Absicht der ursprünglichen Facebook-Vision.

Im Jahre 2005 wurde YouTube als erstes und größtes Videoportal veröffentlicht. 2006 zog Twitter mit den Hashtags und den 140-Zeichen-Kurznachrichten nach.[3]

3.2. Online-Kommunikation

In diesem Unterkapitel wird aufgezeigt, was genau Online-Kommunikation bedeutet und welche Instrumente dafür benutzt werden.

2011 definierten Fraas, Maier und Pentzol das Wort Online-Kommunikation. „Online-Kommunikation ist an die mediale Vermittlung durch vernetzte Computer gebunden und findet auf Basis des Internets statt. (…) Der Begriff des Online-Mediums verweist (…) sowohl auf die technischen Gegebenheiten als auch auf die soziale Dimension des Internet. (…) Vernetzte Computer dienen hierbei als massenmediale Abrufmedien, als teilweise öffentliche Kommunikationsmedien oder als private Kommunikationsmedien“. [4]

Zwei weitere Philosophen (Morris und Organ) definierten die Online Kommunikation anhand mehrerer Faktoren. Als Ordnungskriterien galten soziale und zeitliche Kriterien. Die zeitlichen Kriterien wurden in synchrone und asynchrone Kommunikationsformen unterschieden und mit der Zahl der Kommunikationspartner verbunden.

[3] http://www1.wdr.de/stichtag/stichtag5210.html
[4] https://koorg.wordpress.com/2014/02/14/begriffsdefinition-digitale-kommunikation-online-kommunikation-social-web/

Im Folgenden findet sich eine Tabelle (Abbildung 1), in der erkennbar ist, wie das Prinzip nach Morris und Organ funktioniert.

Sozialdimension Konfiguration	Zeitdimesnion synchron	asynchron
one-to-one	Instant Massaging, Online Spiele	E-Mail, FTP, WWW
one-to-few	Instant Massaging, Online Spiele	Mailinglist, Blog
one-to-many	Online Spiele	WWW, FTP, Mailinglist, Blog
many-to-one		WWW, FTP
many-to-many	Online Spiele	Usenet, Bulletin Board System

Systematisierung der Online-Kommunikation nach Morris & Ogan (1996)

Abbildung 1: Tabelle Online - Kommunikation

Aus dieser Tabelle ist ersichtlich, dass die „Sozialdimension Konfiguration“ fünf Formen der Kommunikation definiert. Die „one-to-one“, die „one-to-few“, die „one-to-many“, die „many-to-one“ und die „many-to-many“. Somit ist die „one-to-one“ Kommunikation auf der synchronen Zeitdimension das Instant-Messaging oder das Online Spiel. Das Instant-Messaging bedeutet einfach erklärt, die direkte Übermittlung von Nachrichten, bei der sich zwei oder mehr Teilnehmer per Textnachricht unterhalten. Dabei löst der Absender die Übermittlung aus.[5]

Auf der asynchronen Zeitdimension lassen sich Email und das WWW als „one-to-one“ Kommunikation definieren. Nimmt man beispielsweise Facebook und einen Prominenten User kann sowohl die Zeitdimension als auch die Sozialdimension unterschiedlich sein. „One-to-many“ ist der Fall, wenn der Prominente Nutzer einen Post schreibt. Die Kommentare die unter seinem Post hinterlassen werden, können sowohl synchron als auch asynchron sein. Eine weitere Form der Sozialdimension wären persönliche Nachrichten.[6] Aufgrund dessen lässt sich klar feststellen, dass nur durch einen einzigen Post mehrere Sozialdimensionen und auch des Öfteren beide Zeitdimensionen vorhandenen sein können. Somit beschränkt sich Online-Kommunikation selten auf nur einen Faktor.

Nun sollen einige Beispiele für Online-Kommunikation genannt werden. Darunter zählen Homepages von Unternehmen, E-Mail Konversation, Kommunikation auf Messengern, Blog Einträge und die Konversation bei Online-Spielen.

[5] http://praxistipps.chip.de/was-ist-instant-messaging-einfach-erklaert_41407
[6] https://koorg.wordpress.com/2014/02/14/begriffsdefinition-digitale-kommunikation-online-kommunikation-social-web/

Der letzte Punkt dieses Unterkapitels sind die sogenannten Push&Pulls. Bei diesen Begriffen geht es darum, wie ein Kunde zu den Informationen eines Unternehmens kommt.

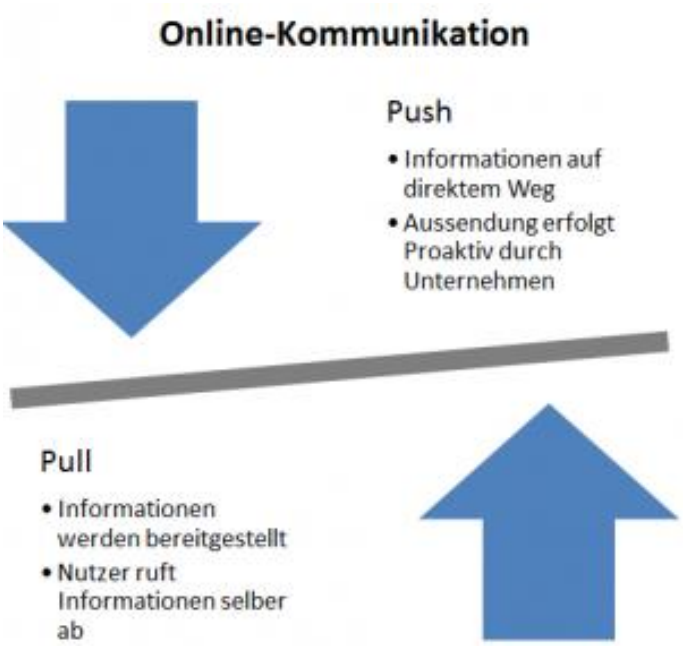


Abbildung 2: Push and Pull Prinzip

Bei einem Kommunikationspull werden die Informationen zur Verfügung gestellt, damit der Kunde oder der Nutzer diese einfach abrufen kann. Diese Informationen befinden sich auf Webseiten, in abonnierten Newslettern oder auf Werbebannern.[7]

Der Kommunikationspush ist eine Form der Online-Kommunikation, bei der der Kunde die Informationen auf direktem Weg erlangt, wie zum Beispiel über TV-Spots oder durch klassische Anzeigen. Nachteil hierbei ist, dass immer mehr Kunden das Interesse an dieser Art der Online-Kommunikation verlieren, da sie selbst entscheiden möchten, wann und welche Informationen für sie abrufbar sind.

3.3. Facebook - Der Ursprung und die Entwicklung

Mark Zuckerberg. Der Mann der „TheFacebook“ gründete und somit eine Revolution der Online-Kommunikation ins Rollen brachte. Der Ursprung der Webseite findet sich in einem Studentenwohnheim in Harvard wieder. Dort wurde „theFacebook“ 2004 von Zuckerburg, Eduardo Saverin, Chris Hughes und Dustin Moskovitz gegründet.[8] Die

[7] http://www.magronet.de/online-kommunikation/
[8] http://www.focus.de/digital/internet/facebook/tid-24930/die-geschichte-des-sozialen-netzwerks-facebooks-eroberung-der-welt_aid_708653.html

Seite konnte damals nicht annähernd die Features bieten die es heute gibt. Jedoch meldeten sich schon am ersten Tag mehr als 600 User von Harvard an. Einen Monat später konnten sich Yale-, Stanford- und Columbia-Studenten ebenfalls anmelden. Ende September 2006 konnten sich auch alle User, die das 13. Lebensjahr vollendet hatten anmelden, Fotos liken und diese mit ihren Freunden teilen. Microsoft kaufte sich 2007 einen Anteil von 1,6 Prozent für 240 Millionen Dollar.

Facebook hat seit 2006 immer wieder große Neuerungen unternommen. Dadurch wuchsen die Mitgliederzahlen stetig. Der Erfolg des Unternehmens lag auch daran, dass seit 2007 Drittanbieter Programme auf der Seite bereitstellen konnten. Im Jahre 2008 konnten die Nutzer von Facebook erstmals miteinander Chatten. Der Facebook-Messenger wurde ins Leben gerufen. Die Nutzung der Plattform ist von Beginn an kostenlos. Geld verdient Facebook mit dem Einblenden personalisierter Werbung.[9] Der größte Umbruch brachte dann die Chronik. Hier wurden die Beiträge wie Tagebucheinträge dargestellt und der zeitliche Ablauf konnte so besser dargestellt werden. Facebook brachte eine grundlegende Neuerung zur Nutzung digitaler Kommunikation. Es erlaubte Nutzern, anders als zuvor, auf direktem Wege Bilder oder Beiträger zu „liken“, zu teilen oder zu kommentieren.

Kritik an Facebook ist aus der Sicht des Datenschutzes geübt worden. Viele behaupten, dass Facebook den Usern nicht klar zu erkennen gibt, was mit ihren Inhalten passiert. Jetzt hat Facebook versucht, mit einem Erklär-Video Zweifel von Kritikern aus dem Weg zu räumen. So wird unter anderem aufgezeigt, dass Fotos von Nutzern nicht Facebook sondern den Nutzern selbst gehören.

Die aktuellsten Zahlen von Juli 2017 zeigen die ungebremste Entwicklung von Facebook. Waren es im Mai 1,936 Mrd. monatlich aktive Nutzer, so wurde im Juli 2017 die zwei Milliarden Marke überschritten. Hier waren es 2,006 Mrd. monatlich aktive Nutzer.[10]Nun wird auch klar, warum Facebook teil dieser Arbeit ist. Das soziale Netzwerk ist das meist genutzte und älteste seiner Art. Aufgrund dessen ist es sinnvoll, dieses Netzwerk herauszunehmen. Vergleicht man Facebook mit Twitter, ist deutlich zu sehen, das Twitter nur 328 Millionen aktive Nutzer im Monat hat[11]. Oder um ein anderes Beispiel zu nennen, Instagram mit 800 Millionen aktiven Nutzern im Monat. [12]Aus der Sicht des Staates und seines Informationsinteresses steht deshalb Facebook sicherlich auch im Vordergrund.

[9] http://www.focus.de/digital/internet/facebook/tid-24930/die-geschichte-des-sozialen-netzwerks-facebooks-eroberung-der-welt_aid_708653.html
[10] http://www.thomashutter.com/index.php/2017/07/facebook-aktuelle-zahlen-zu-facebook-q22017/
[11] https://de.statista.com/statistik/daten/studie/232401/umfrage/monatlich-aktive-nutzer-von-twitter-weltweit-zeitreihe/
[12] https://allfacebook.de/instagram/instagram-nutzer-deutschland

3.4. WhatsApp - Geschichte und Übernahme

Im Folgenden wird die Geschichte von Jan Koum genauer erläutert. Er ist der Erfinder des zweitgrößten Messeging-Dienstes für mobile Endgeräte. Koum wuchs in der Nähe von Kiew (Ukraine) in ärmlichen Verhältnissen auf. Nach dem er die Highschool absolviert hatte, ging er auf ein College nach San Jose und nicht wie Facebook Gründer Mark Zuckerberg nach Harvard.[13] Kurze Zeit später warf er sein Studium hin. Danach kam er über Umwege zu Yahoo. Im Jahr 2007 verließ er Yahoo wieder und 2009 kaufte er sich sein erstes iPhone, das ihm die Idee für Statusmeldungen neben Kontakten brachte. Kurze Zeit später gründete er die Firma „WhatsApp Inc“. Den Namen hatte er durch „whats up“, dem englischen für „was geht“ gewählt. Aus „whats up“ wurde dann „WhatsApp“. Koum schaffte durch WhatsApp eine neue Kommunikationsrevolution. Im Juni 2009 erlaubte Apple, Push-Benachrichtigungen auf WhatsApp zu verwenden. Dies bedeutet, dass jedes Mal, wenn ein Status geändert wurde, alle anderen Kontakte die Änderungen sofort zu sehen bekamen. Somit wurde WhatsApp zu einem Instant-Messaging.[14] Neben Push-Benachrichtigungen konnten die Nutzer in einer für sie geschlossenen Plattform innerhalb eines ständigen Rahmens in Verbindung bleiben und Informationen austauschen.

Anders als bei Facebook kann man allerdings bei WhatsApp den Status weder liken, teilen oder kommentieren. Bei der Veröffentlichung war WhatsApp ohne Konkurrenz. Dies erklärt unter anderem das große und stetige Wachstum. Als WhatsApp 2.0 veröffentlicht wurde, gab es bereits 250.000 Nutzer. Heute hat WhatsApp rund 1,3 Milliarden Nutzer[15] und ist somit hinter Facebook. Dies beantwortet ebenfalls die Frage, warum auch WhatsApp Gegenstand der Arbeit ist. 2014 wurde WhatsApp von Facebook gekauft. Der Preis betrug 19 Milliarden US-Dollar. Ziel von Zuckerberg war es, die ganze Welt noch mehr zu vernetzen. Und dies sollte mit WhatsApp möglich werden.

Was das staatliche Informationsinteresse betrifft, so ist wichtig, dass im Rahmen von WhatsApp der Tendenz nach, Mitteilungen persönlicher und privater Art noch von größerer Bedeutung sind als bei Facebook.

[13] http://www.stern.de/digital/smartphones/jan-koum-die-unglaubliche-erfolgsgeschichte-des-whatsapp-gruenders-3411916.html
[14] http://www.stern.de/digital/smartphones/jan-koum-die-unglaubliche-erfolgsgeschichte-des-whatsapp-gruenders-3411916.html
[15] https://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/

3.5. Differenzierung der Überwachung je nach Form der Kommunikation?

Für den Staat stellt sich die Frage, welche Formen der Kommunikation für seine Zwecke der Überwachung besonders wichtig oder auch unwichtig sind. Indes dürfte eine Differenzierung der staatlichen Überwachung je nach dem Medium kaum praktikabel sein. Es lässt sich nämlich verallgemeinernd nicht sagen, welche speziellen Inhalte in welchem Medium generell im Vordergrund stehen und deshalb stark oder weniger stark überwacht werden sollen. Zur Durchführung des Informationsinteresses des Staates bedarf es deshalb im Grundsatz der Überwachung alle Formen der Kommunikation. Die Abwägung zwischen dem Informationsinteresses des Staates und dem Interesse an einer freiheitlichen Gesellschaft wird aus diesem Grund für alle Formen der Kommunikation im Prinzip in gleicher Weise vorzunehmen sein.

4. Informationelles Selbstbestimmungsrecht in Deutschland

Nachdem im vorherigen Kapitel die heutigen Arten digitaler Kommunikation erörtert worden sind, wendet sich die vorliegende Arbeit vor diesem Hintergrund der Frage zu, wie sich diese modernen Formen der Kommunikation aus der Sicht einer freiheitlichen Ordnung des Staates darstellen. Im Vordergrund steht das Konzept und der Begriff der informationellen Selbstbestimmung, wie er vom Bundesverfassungsgericht geprägt worden ist und unser heutiges Rechtsverständnis bestimmt.

Im folgenden Kapitel soll aufgezeigt werden, was das informationelle Selbstbestimmungsrecht ist, woraus es sich zusammen setzt und wie Überwachung und die Artikel 1 und 2 im Grundgesetz miteinander vereinbar sind. Des Weiteren soll der Roman „1984“ von George Orwell mit der heutigen Situation verglichen werden.

Das Informationelle Selbstbestimmungsrecht ist einfach ausgedrückt, jeder Mensch darf selbst über die Verarbeitung und Preisgabe seiner eigenen Daten bestimmen.[16] Das Recht ist im Grundgesetz nicht ausdrücklich erwähnt, es ergibt sich jedoch aus dem Grundgesetzbuch Artikel 1, Absatz 1 (Würde des Menschen) und Artikel 2, Absatz 1 (Freiheit des Menschen), dem sogenannten „allgemeinen Persönlichkeitsrecht“.[17]

Erstmals erwähnt wurde das Selbstbestimmungsrecht 1984 bei der Volkszählung. Hier sollten neben Statistiken auch Angaben zu Wohnort und Einkommen der Bürger gemacht werden. Abgeleitet auf das moderne Informationszeitalter entstand so, das informationelle Selbstbestimmungsrecht. Würde es das Selbstbestimmungsrecht nicht geben, bestünde die Gefahr, dass sich aus einer Vielzahl einzelner personenbezogener Daten ein ganzes Persönlichkeitsprofil zusammensetzen ließe und dies eine Gefährdung und massive Einschränkung für den Einzelnen darstellen würde.

Ein Eingriff in das informationelle Selbstbestimmungsrecht existiert dann, wenn Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten ohne Einverständnis der betroffenen Personen unternommen werden. Jeder Eingriff in das Recht der informationellen Selbstbestimmung muss durch eine gesetzliche Grundlage gestattet werden, die den Zweck der Datenerhebung klar erkennen lässt. Außerdem sind Einschränkungen wenn überhaupt nur im überwiegenden Allgemeininteresse zulässig.

[16] http://www.bpb.de/nachschlagen/lexika/recht-a-z/22392/informationelle-selbstbestimmung
[17] http://alt.staatundverwaltung.jura.uni-leipzig.de/sites/uni-leipzig.de.enders/files/Das%20Grundrecht%20auf%20informationelle%20Selbstbestimmung.pdf

4.1. Würde des Menschen

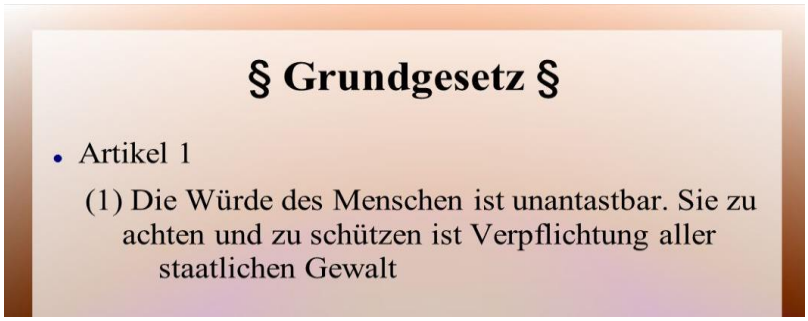
Was bedeutet die Würde des Menschen und welche Maßnahmen gefährden dieses Grundrecht? Diese Fragen werden nun erläutert.

Als Würde des Menschen versteht man, dass alle Menschen - unabhängig von Geschlecht, Herkunft oder Alter - denselben Wert haben und dass dieser Wert über dem aller anderen Lebewesen und Dingen steht. Die Verankerung im Grundgesetz geht auf die massive Missachtung der Menschenwürde während des Nationalsozialismus zurück. Dieser Artikel macht deutlich, dass der Staat alles zu unterlassen hat, was die Menschenwürde beeinträchtigen könnte. Der Staat hat die Menschenwürde zu achten und zu schützen.

Die Menschenwürde ist sowohl ein Abwehrrecht gegen die öffentliche Gewalt selbst, als auch ein Leistungsrecht. Das bedeutet, das der Gesetzgeber verpflichtet wird, allgemeinverbindliche Normen zu erlassen, die dem Schutz der Menschenwürde dienen.[18]

Verstöße gegen die Menschenwürde sind also beispielsweise Rufschädigung oder Diskriminierung. Auch die Verwendung als bloßes Mittel zum Zweck - wie es bei der Überwachung der Fall ist - ist ein Verstoß. In Kapitel 3.3 soll dies genauer erläutert werden.

Abbildung 3: Grundgesetz Artikel 1, Absatz 1



[18] https://www.grundrechteschutz.de/gg/menschenwurde-2-255

4.2. Freiheit des Menschen

Im Grundgesetz Artikel 2 steht: „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.“[19]Dies ergibt sich aus dem Menschenbild, welches dem Grundgesetz zugrunde liegt.

Somit ist das Recht auf Freiheit der Menschen in drei Erscheinungsformen gewährleistet: Das Recht auf die freie Entfaltung der Persönlichkeit, das Recht auf körperliche Unversehrtheit und Leben und das Recht auf Freiheit der Person.

Das Recht auf freie Entfaltung der Persönlichkeit umfasst Handlungsfreiheiten wie Vertragsfreiheit oder Wettbewerbsfreiheit. Es umfasst auch das Selbstbestimmungsrecht. Eine Einschränkung findet nur durch die Rechte anderer, das Sittengesetz und die verfassungsmäßige Ordnung statt.[20]

Das Recht auf körperliche Unversehrtheit schützt vor jeglichen Eingriffen, die die Gesundheit des Menschen beeinträchtigen. Als letzte Erscheinungsform gilt die Freiheit der Person. Dies bezieht sich auf die körperliche Bewegungsfreiheit jedes Einzelnen.

Im Hinblick auf diese Betonung der Freiheit stellt sich die Frage, wie der Schutz dieser Freiheit im Kontext der modernen Kommunikation und ihrer Überwachung durch den Staat gewährleistet werden kann.

[19] https://www.gesetze-im-internet.de/gg/art_2.html
[20] http://www.grundrechtefibel.de/fibel_freiheitsrechte.html

4.3. Abschreckende Wirkung auf die Würde und Freiheit der Menschen im Rahmen der uneingeschränkten Überwachung

In diesem Unterkapitel wird erläutert, warum Überwachung nicht mit dem Grundgesetz vereinbar ist, obwohl das Recht auf Selbstbestimmung nicht explizit verankert ist.

Wie schon in Kapitel 3.1 und 3.2 aufgeführt, hat jeder Mensch sowohl das Recht auf seine Würde als auch seine Freiheit. Der Staat hat sowohl die Aufgabe, die Menschenrechte zu achten als auch zu schützen. Dies gilt auch, obwohl die Grundrechte im Allgemeinen nur im Verhältnis zwischen Staat und Bürger ihre Wirkung entfalten („Drittwirkung der Grundrechte“). Hierbei bedeutet „Drittwirkung“ auch der Schutz vor einem ausländischen Geheimdienst, einem inländischen Geheimdienst oder aber auch privaten Unternehmen.

Der Mensch ist ein frei entscheidungsfähiges, handelndes Individuum. Wird er überwacht, ohne davon Kenntnis zu haben, kann dies ein Verstoß gegen seine Menschenwürde darstellen. [21]

Doch wird bei der Überwachung das Recht auf Freiheit ebenfalls verletzt? Die Antwort findet sich im Grundgesetz. Das Recht auf Privatsphäre und das Recht auf Handlungsfreiheit wird bei der staatlichen Überwachung nicht gewährleistet. Die Privatsphäre ist für die freie Entfaltung der Persönlichkeit extrem wichtig und dieses Grundrecht muss sowohl vom Staat als auch von Dritten gewährleistet werden.

[21] https://andreasvongunten.com/blog/201378uberwachung-respektiert-die-wurde-des-menschen-nicht-html/

5. Die Folgen übermäßiger Überwachung auf das Verhalten des Einzelnen

In den vorangegangenen Kapiteln wurde erläutert, was die Rolle des Selbstbestimmungsrechtes im Fall der totalen Überwachung ist. Jeder hat das Recht, über seine Daten zu bestimmen. Doch was geschieht, wenn die Überwachung in Deutschland zunimmt und - genau wie in den USA - Kameras installiert werden, Facebook-Konten überwacht werden oder Telefonate ohne wirklichen Grund abgehört werden? Das Jetzt sieht nicht ganz so schlimm aus, jedoch lauert die Gefahr der Überwachung überall. Die Folgen dessen sollen nun geschildert werden. Des Weiteren wird es einen Einblick in das Volkszählungsurteil 1983 vom Bundesverfassungsgericht geben.

Die Folgen der Überwachung sind breit gefächert. Wie schon erwähnt werden die Grundrechte der Menschen verletzt, wenn ohne deren Wissen, geheime und persönliche Daten ausgespäht werden. Artikel 2 im Grundgesetz behandelt ebenfalls die Handlungsfreiheit. Wenn sich Personen ständig Gedanken darüber machen, ob oder dass sie Überwacht werden, so passen sie auch automatisch ihr Verhalten an. Sie geben darauf Acht, was sie zu wem sagen oder auch auf den sozialen Netzwerken kommunizieren. Dieses Verhalten passen sie jedoch nur aus Angst an.[22] Der Fachbegriff hierfür nennt sich „Chilling Effect“. [23] Auch die Privatsphäre wird eingeschränkt, was ein Verstoß gegen die Grundrechte bedeutet. Wenn sich Individuen aus Angst vor der Überwachung verunsichert fühlen und sich nicht trauen, ihre Rechte geltend zu machen oder frei ihre Meinung äußern zu dürfen, schränkt dies nicht nur die Privatsphäre sondern auch die freie Entfaltung der Persönlichkeit ein. Durch die Einschränkungen trauen sich die Menschen ebenfalls nicht mehr, ihren Glauben oder ihre Ansichten laut zu artikulieren, obwohl dies im Grundgesetz Artikel 4 (Die Freiheit des Glaubens ist unantastbar) verankert ist.[24] Der Mensch fühlt sich unter solchen Umständen nicht mehr frei. Durch diese Einschränkungen wird auch das Gemeinwohl beeinträchtigt, da ein freiheitlich demokratisches Gemeinwesen der selbstbestimmten Mitwirkung seiner Bürger eine Notwendigkeit ist. Bedeutet also, das die Demokratie durch die Überwachung der Social-Media-Kommunikationgefährdet ist. Die Tatsache, dass niemand mehr seine Rechte geltend macht und Angst hat, beschrieb auch George Orwell in seinem Roman „1984“. Hierbei geht es um eine düstere Vision eines Überwachungsstaates. Er beschreibt unter anderem die langsame Ergreifung der Gedankenkontrolle durch die Reduzierung von Sprache in Zeitungsartikeln, sodass der Gedankenspielraum zunehmend eingeschränkt wird. Im Buch wird geschildert, wie der Überwachungsstaat aussieht. Ständige Überwachung durch Fernseher und Telefone.

[22] https://openjur.de/u/268440.print
[23] http://www.sueddeutsche.de/digital/privatsphaere-das-internet-ein-ueberwachtes-zuhause-1.1746611-2
[24] https://openjur.de/u/268440.print

Orwell beschreibt ebenfalls, die Angst der Überwachung und somit das Anpassen an das System. Orwell zeigt also, die Vision - oder die Horrorvision - einer vom Staat absolut kontrollierten und überwachten Gesellschaft.

Dass Deutschland beim Thema Überwachung empfindlich ist, geht auf unsere Geschichte zurück. Im dritten Reich hatte die Staatssicherheit Zugriff auf alle Telefonate, Briefe und sonstige Kommunikation der Bevölkerung. Dabei wurde massiv gegen die Grundrechte des Menschen verstoßen. Das könnte auch erklären, warum Deutschland mit der Überwachung anders umgeht als zum Beispiel die Amerikaner. Immer mehr Menschen in den USA stimmen für Überwachungskameras und das Abhören von Telefonaten. Denn nur so kann angeblich Sicherheit garantiert werden.[25] Wichtig ist zu erwähnen, dass der technische Fortschritt zwei Seiten hat. Eine positive, nämliche die Chance der Vernetzung und einmal die negative Seite. Diese ist das Risiko der Datensammlung. Das bedeutet, die sozialen Netzwerke speichern täglich die Daten junger Nutzer in der bekannten I-Cloud. Aus diesen Daten wird eine Großdatensammlung über jeden Nutzer erstellt. Dies bedeutet, dass allein durch die Speicherung des Internetverkehrs oder der Kommunikation zwischen A und B ein ganzes Persönlichkeitsprofil erstellt werden kann, was wiederum zur Folge hat, dass die Privatsphäre kaum noch existent ist.

Bedenkt man die Großdatensammlung in den sozialen Netzwerken, so stellt sich in besonderer Weise die oben schon aufgezeigte Frage: Unsere Grundrechte wenden sich eigentlich gegen den Staat an sich. Doch sind diese Rechte heutzutage nicht mehr gefährdet durch die Spionage von Dritten? Hierbei sind „dritte“ nicht nur die NSA oder andere ausländische Geheimdienste. Damit sind auch Ehefrau und Nachbar gemeint, die sich gegenseitig und ohne Wissen der anderen ausspionieren.

Das Bundesverfassungsgericht verabschiedete das sogenannte Volkszählungsurteil von 1983. Darin sind alle Folgen der Volkszählung auf die Folgen der totalen Überwachung übertragbar. Das heißt auch, dass die Daten nur für das eigentliche Ziel verwendet werden dürfen und nicht an Dritte weiter gereicht werden können.[26]

[25] http://www.tagesspiegel.de/meinung/usa-und-ueberwachung-warum-es-moralisch-sein-kann-die-eigenen-buerger-auszuspaehen/8334518.html
[26] https://openjur.de/u/268440.print

6. Staatliche Überwachungsorganisationen im Innland und im Ausland

In diesem Kapitel geht es darum, die vier großen staatlichen Überwachungsorganisationen National Security Agency (kurz: NSA), Central Security Agency (kurz: CIA), den Bundesnachrichtendienst (kurz: BND) und den Bundesverfassungsschutz (BfV) genauer zu untersuchen. Des Weiteren sollen Beispiele für Überwachungsarten erläutert und die Zusammenarbeit von staatlichen Überwachungsorganisationen mit Unternehmen analysiert werden.

6.1. National Security Agency

Die NSA ist nicht nur eine der größten Überwachungsorganisationen weltweit. Nein, sie hat auch für einen der größten Überwachungsskandale gesorgt. Edward Snowden, ein ehemaliger Mitarbeiter sorgte 2014 für einen Weltweiten Skandal. Doch bevor dies verdeutlicht wird, sollten zunächst die Einrichtung und Hintergrundinformationen der NSA dargestellt werden.

Die National Security Agency (im weiteren NSA) wurde 1945 unter US-Präsident Harry Truman als Unterabteilung des Verteidigungsministeriums der Vereinigten Staaten gegründet. Ursprünglich wurde die NSA als ASA betitelt. Army Security Agency.[27] Nachdem im November 1952 Dwight D. Eisenhower zum Präsident der Vereinigten Staaten gewählt worden war, wurde die NSA offiziell gegründet, mit dem Ziel, Aufklärung durch technische Medien zu realisieren. Dazu gehören auch das Abhören ausländischer Nachrichtendienste. Erster Direktor 1952 war Joseph N. Wenger. Seit 2014 ist Richard H. Ledgett Direktor der NSA.

Die NSA ist Mitglied in der „Intelligence Community“, sie ist aber selbstständig und nicht Teil der CIA. (Zusammenschluss aller US-Nachrichtendienste) und arbeitet auch mit Geheimdiensten befreundeter Staaten zusammen. Mit der Zeit entwickelte die NSA ihre Überwachungstechniken so perfekt, dass eine Abwehr immer schwieriger wurde.

Der Hauptsitz der NSA ist in Maryland. Es ähnelt einer kleinen Stadt. „Crypto City“ genannt. Mit eigener Auffahrt befindet sich hier die Überwachungszentrale, insgesamt 5 Gebäude, einer eigene Schule, einer Wintersportanlage und einer Redaktion für die eigene Tageszeitung.

[27] http://www.giga.de/unternehmen/nsa-was-ist-die-national-security-agency-eigentlich/

Abbildung 5: Crypto City - Hauptquartier der NSA

Außenstellen hat die NSA auf Hawaii und in Deutschland. Konrad Adenauer unterschrieb einen Überwachungsvorbehalt, der den ehemaligen Besatzungsmächten weiterhin erlaubte, elektronische Daten zu sammeln.

2013 sorgte Edward Snowden für den größten Überwachungsskandal den es jemals gegeben hat. Er war ehemaliger Mitarbeiter der NSA und veröffentlichte streng geheime Informationen über seinen ehemaligen Arbeitgeber. So wurde veröffentlicht, dass die NSA nahezu jeden abhören würde und alle elektronischen Wege jedes einzelnen speichern und auswerten würde. Laut Snowden leitete der BND Verbindungsdaten von Telefonaten, SMS oder E-Mails an eine der Außenstellen der NSA weiter.

Zuletzt zählte die NSA 40.000 Mitarbeiter mit einem Budget von 10,8 Milliarden US-Dollar[28].

[28] http://www.t-online.de/nachrichten/specials/id_64763512/nsa-us-geheimdienst-kann-laut-guardian-fast-alles-ausspaehen.html

6.2. Central Intelligence Agency

Die CIA ist der Auslandsgeheimdienst der Vereinigten Staaten. Die NSA beschafft sich ihre Daten durch Signals Intelligence (Informationsbeschaffung durch Technik), während die CIA ihre Informationen vorwiegend von und durch Menschen bekommt. Jedoch ist der Geheimdienst nicht nur für die Beschaffung und Auswertung von elektronischen Daten zuständig, er ist ebenfalls für Geheimoperationen im Ausland autorisiert.

Gründung der CIA erfolgte am 18.9.1947. Roscoe Hillenkoetter wurde kurz darauf zum ersten Direktor ernannt. [29]Ziel war es, illegale Informationen von anderen Staaten zu erlangen. Dies geschah unter anderem durch die Zusammenarbeit mit der NSA. Ende 1950 begann die CIA mit Spionageflügen in fremdem Luftraum. Während des Vietnamkrieges zum Beispiel leitete die CIA mehrere geheime Operationen in Kambodscha oder Nordvietnam. Seit 2004 ist die CIA auch für Operationen mit Drohnen verantwortlich. Dieses Jahr erlaubte Präsident Trump der CIA, Terroristen durch Drohnen zu töten.[30] Hauptsitz der CIA ist in Langley,Virginia, wo all die von Agenten gesammelten Daten ausgewertet werden.

Die CIA ist in fünf Abteilungen gegliedert. Die Auswertung (Intelligence), die Beschaffung (National Clandestine Service), Technische Beratung (Science and Technology), Verwaltung (Support) und Leitung (Office).[31]

Die Zahl der Mitarbeiter in der CIA liegt laut Angaben der Presse bei 20.000.[32]Bei dem Budget das der CIA jährlich zur Verfügung steht, handelt es sich um eine Summe von 10,3 Milliarden Dollar (Stand 2013), im Vergleich zu etwa 800 Millionen des BND. Diese Aussage stammt von Whistleblower Edward Snowden.[33]

[29] http://www.dieterwunderlich.de/cia.htm
[30] https://deutsche-wirtschafts-nachrichten.de/2017/03/19/us-praesident-trump-erlaubt-der-cia-das-toeten-mit-drohnen/
[31] http://www.sueddeutsche.de/politik/geheimdienste-im-ueberblick-der-maechtige-graue-staat-der-usa-1.1820288
[32] http://diepresse.com/home/ausland/aussenpolitik/1438653/Von-NSA-bis-CIA_Die-maechtigen-USGeheimdienste#slide-1438653-3
[33] http://www.focus.de/politik/ausland/usa/cia-bekommt-groesste-summe-neue-snowden-enthuellung-verraet-budget-der-us-geheimdienste_aid_1085776.html

6.3. Bundesnachrichtendienst

Der Bundesnachrichtendienst (folgend BND) ist ein deutscher Auslandsnachrichtendienst der 1956 gegründet wurde. Dieser ist neben dem Bundesamt für Verfassungsschutz und dem Bundesamt für den Militärischen Abschirmdienst einer der drei deutschen Nachrichtendienste des Bundes. Für die Informationsbeschaffung hat der BND vier Möglichkeiten. „HUMINT“, „SIGINT“, „IMINT“ und „OSINT“. HUMINT bedeutet Human Intelligence. Also die Informationsgewinnung durch menschliche Quellen. „SIGNIT“ steht für Signal Intelligence. Hier werden die Datenströme gefiltert und nach bestimmten Inhalten untersucht. Bei der Imagery Intelligence (IMINT) geht es um die Gewinnung von Informationen durch Luftbilder. Bei der letzten Möglichkeit, der „OSINT“, werden die Informationen durch frei zugängliche Informationskanäle beschafft. Es ist also die Variante der Open Source Intelligence. Der BND ist dem Kanzleramt unterstellt und für die Auslandsaufklärung zuständig. Erster Präsident war Reinhard Gehlen, der unter anderem die Aufklärung der militärischen Lage voran trieb. Neben der Informationsbeschaffung durch menschliche Quellen wurde die Aufklärung auch durch technische Mittel immer wichtiger.[34]

Im Oktober 1963 wurde ein Kabinettausschuss für Fragen des geheimen Nachrichtenwesens und Sicherheit gebildet. 1969 wurde der Hauptsitz des BND in Pullach erbaut. 1972 weitete der BND sein Aufgabenspektrum auf die nachrichtendienstliche Aufklärung von Terrorgruppen aus. Ab 1978 regelte das parlamentarische Kontrollgremium die Tätigkeiten der Nachrichtendienste des Bundes. Am 20. Dezember 1990 verabschiedete der Bundestag das Gesetz über den Bundesnachrichtendienst. Darin waren Aufgaben und Befugnisse des BND unter Berücksichtigung datenschutzrechtlicher Belange festgelegt.[35]Im August 2001 wird eine eigene Abteilung zur Aufklärung des internationalen Terrorismus eingerichtet. Laut Daten von Snowden haben BND und NSA zusammengearbeitet. Hierbei sollte der BND die Gesetze der Privatsphäre aufweichen, damit es bessere Möglichkeiten für den Austausch von geheimdienstlichen Informationen geben würde. [36] Der BND beschäftigt circa 6500 Mitarbeiter mit einem Jahresbudget von 832,8 Millionen Euro.

[34] http://www.bnd.bund.de/DE/Organisation/Geschichte/Geschichte_Ueberblick/Timeline_node.html;jsessionid=69F43E42964C99C2C81359101F4C28CB.1_cid386
[35] http://www.bnd.bund.de/DE/Auftrag/Informationsgewinnung/HUMINT/humint_node.html
[36] http://www.spiegel.de/media/media-34000.pdf

6.3.1. Datenschutz

Im Folgenden soll ein kleiner Überblick darüber gegeben werden, welche Möglichkeiten der Datenschutz zur Abwehr einer Überwachung durch den Nachrichtendienst gibt. Das Gesetz über den BND aus dem Jahre 1990 besteht in großem Umfang aus Regelungen zum Datenschutz.

Grundsätzlich wird Datenschutz als Recht verstanden, eigene Entscheidungen über Verwendung und Sammlung seiner Daten zu treffen. Der Datenschutz soll in der heutigen Zeit der totalen Überwachung entgegenwirken. Wer gegen diesen Schutz verstößt, verletzt die Persönlichkeitsrechte.

Der Datenschutz in den USA ist kaum gesetzlich geregelt. Auf den BND bezogen ist wichtig zu erwähnen, dass die Informationsbeschaffung durch den BND nur im Rahmen der Vorschriften über den Datenschutz gestattet ist. Dies bedeutet, die Informationen, die Mitarbeiter von Menschen bei Befragungen erhalten, sind legal und dürfen verwendet werden. Laut dem BND-Gesetz werden beim Einsatz technischer Hilfsmittel zur Informationsbeschaffung keine personenbezogenen Daten erhoben und keine IP-Adresse gespeichert[37]. Das Parlamentarische Kontrollgremium ist für bestimmte Überwachungsmaßnahmen von Brief- Post- und Fernmeldegeheimnisse zustimmungspflichtig. Das Abhören und Speichern von personenbezogenen Daten ist nur dann legal, wenn es zur Erfüllung der Aufgaben des Nachrichtendienstes erforderlich ist.[38] Um ein Beispiel zu nennen, der Schutz unserer Sicherheit. Es trifft als nicht zu, das der BND, wenn er sich an das geltende Recht hält, ohne jede Einschränkung tätig werden darf.

Wenn man seine Daten im Internet wirklich schützen will sollte man einiges beachten. Zum einen ist es wichtig, personenbezogene Daten wie Anschrift, Telefonnummer, etc. nicht im Internet zu speichern und solche Daten möglichst zu schützen. Des Weiteren kann jeder Nutzer im Internet selbst festlegen, welche Daten er in den sozialen Netzwerken veröffentlichen will[39]. Ebenfalls ist wichtig, auf Facebook, seine Religiösen oder Politischen Ansichten nicht mit der Öffentlichkeit zu teilen, da Dritte (ob Überwachungsorganisation oder Bekannte) diese Informationen dann ebenfalls erhalten.

Um überhaupt zu verhindern, das ein Verstoß gegen den Datenschutz eintritt, sollten die Passwörter zum einen nicht gespeichert werden und zum anderen möglichst kryptisch und mit viel Abwechslung gebildet werden. Auch empfiehlt es sich, seine Passwörter mehrmals zu ändern[40].

---

[37] http://www.gesetze-im-internet.de/datenschutz.html
[38] http://www.gesetze-im-internet.de/bndg/__19.html
[39] http://www.silver-tipps.de/datenschutz-im-internet-kurz-und-knapp-ein-ueberblick/
[40] https://www.selbstdatenschutz.info/digitale_selbstverteidigung

6.4. Bundesamt für Verfassungsschutz

Der Bundesverfassungsschutz ist ein Inländischer Nachrichtendienst, dessen wichtigste Aufgabe es ist, Überwachungen von möglichen Bedrohungen der Interessen gegen die Bundesrepublik Deutschland zu gewährleisten. [41]

Das Bundesamt für Verfassungsschutz untersteht dem Bundesinnenministerium und wird von einem Präsidenten geleitet. Gründung des BfV war 1950. Die Aufgaben wurden unter anderem mit Überwachungen von Brief- und Telefonverkehr erledigt. Die Kontrolle darüber hatte ein parlamentarisches Gremium. Dieses Gremium ist ebenfalls für den BND zuständig. Der Verfassungsschutz gewinnt seine Informationen aus offenen und zugänglichen Quellen.[42]

Der BfV wird durch verschiedenste Institutionen und auf verschiedenen Ebenen kontrolliert. Insgesamt gibt es vier Ebenen. Diese sind: Verwaltungskontrolle, Parlamentarische Kontrolle, gerichtliche Kontrolle und öffentliche Kontrolle. Die Verwaltungskontrolle hat die Aufgabe, die Umsetzung von Datenschutzvorschriften und die Einhaltung von Dienstvorschriften zu überwachen. Bei der Parlamentarischen Kontrolle ist es das Ziel, die drei Nachrichtendienste in Deutschland zu kontrollieren. Dies erfolgt durch Akteneinsicht, sämtliche Befragungen der Angehörigen von Mitarbeitern und den unbeschränkten Zugang zu allen Institutionen. Bei der gerichtlichen Kontrolle ist jedes Handeln des BfV durch ein unabhängiges Gericht durch einen Antrag hin überprüfbar.[43]Im weitesten Sinne ist es auch die Aufgabe der Medien, durch Recherche und Berichterstattung die Öffentlichkeit zu informieren und auf diese Weise ebenfalls eine Kontrollfunktion auszuüben.

2015 waren im BfV rund 2900 Mitarbeiter angestellt. Das Budget lag bei 348 Millionen Euro.

[41] https://www.verfassungsschutz.de/de/das-bfv/aufgaben/was-genau-macht-der-verfassungsschutz
[42] https://www.verfassungsschutz.de/de/das-bfv/aufgaben/was-genau-macht-der-verfassungsschutz
[43] https://www.verfassungsschutz.de/de/das-bfv/aufsicht-und-kontrolle

6.5. Arten der Überwachung

Im folgenden Kapitel werden 3 Arten der Überwachung beschrieben, die NSA und andere Geheimdienste nutzen. Die vier zu erklärenden Programme sind PRISM, Tempora und XKeyscore. Des Weiteren soll verdeutlicht werden, was Facebook, Google und Microsoft mit dem PRISM-Programm zu tun haben.

6.5.1. PRISM-Programm

Das PRISM-Programm wurde laut Snowden 2007 ins Leben gerufen und beschreibt die totale Überwachung von Telefondaten, Internetdaten wie Videos, Fotos, Emails, Chats etc., sowie Daten von WhatsApp und Standortbestimmungen von Smartphones.

PRISM soll dabei helfen, Personen zu überwachen, die im In- und Ausland miteinander digital kommunizieren. Laut Snowden kann die NSA somit auf alle Kommunikationsvorgänge von Facebook, Google, Yahoo und Microsoft zugreifen. Die betroffenen Firmen dementierten zu einem späteren Zeitpunkt, dass die Daten ohne ihres Wissens weiter geleitet wurden.[44]

2014 kündigte Obama einige Einschränkungen des Programs an. Unter anderem sollten Telefondaten nur noch unter richterlicher Anordnung oder im Notfall erlaubt sein. Ebenfalls sollte die Öffentlichkeit mehr über die Aktivitäten der Geheimdienste informiert werden. Diese Schutzmaßnahmen sollten jedoch nur für die US Bürger gelten. Laut dem britischen „Guardian“ wurden in Deutschland ebenfalls in hohem Maße Telefon- und Internetdaten ausspioniert.[45]

6.5.2. Tempora

Eine andere Überwachungsart ist Tempora. Diese wird vom britischen Geheimdienst Government Communication Headquaters (GCHQ) benutzt. Das Programm soll seit 2011 aktiv sein. Tempora dient ebenfalls dazu, Telefonate und Internetdaten von der Bevölkerung zu überwachen. Jedoch ist Tempora noch weitaus umfangreicher als PRISM.[46] Dies liegt daran, dass das Programm die transatlantischen Glasfaserkabel anzapft und somit 600 Millionen Verbindungen täglich abhören kann.

Die Daten der Überwachung werden dann bis zu 30 Tagen gespeichert. Auch werden E-Mails, Einträge in sozialen Netzwerken und persönliche Daten von Internetnutzern ausgespäht.

---

[44] http://www.secupedia.info/wiki/PRISM_und_Tempora
[45] https://web.archive.org/web/20130828010839/http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining#
[46] http://www.secupedia.info/wiki/PRISM_und_Tempora

Sowohl Tempora als auch PRISM sollen zu einem Geheimdienstprojekt von fünf Staaten gehören,(Großbritannien, USA, Kanada, Australien und Neuseeland) genannt „five eyes“. Deutschland ist daran nicht beteiligt.

6.5.3. X-Keyscore

Das Spähprogramm X-Keyscore unterscheidet sich stark von PRISM und Tempora. Das Programm wurde 2006 entwickelt und 2007 hatte die NSA 850 Milliarden Anrufdaten und 150 Milliarden Internetdaten auswerten können.[47]Für diese Tätigkeit werden die modernsten technischen Mittel, vor allem die Leistungsfähigsten Computer eingesetzt.

Es ist für die Überwachung und Durchsuchung von Daten im Internet zuständig. Mit dem Unterschied, dass das Programm die Internetaktivität von Nutzern in Echtzeit überwacht.

Dies bedeutet, das E-Mails die gesendet wurden, oder Suchanfragen die auf Amazon aufgegeben wurden, direkt von der NSA erfasst und ausgewertet werden können[48]. Des Weiteren dient die Software dazu, Verdächtige zu entdecken, die bisher noch nicht auf dem Schirm waren. Durch die „Verschlagwortung“ bei der Auswertung der Daten, können NSA-Mitarbeiter E-Mail Adresse, Name und Zeitraum in ein Suchfeld eingeben, sodass die gesuchte E-Mail zum Vorschein kommt und erneut Daten erfasst werden können. So funktioniert ebenfalls die Überwachung von Facebook-Konversationen.

Abbildung 6: Einsatz X-Keyscore

[47] http://www.webcitation.org/6IZA2XyBg
[48] https://www.welt.de/politik/deutschland/article118593621/So-funktioniert-das-XKeyscore-Programm-der-NSA.html

6.6. Staatliche Überwachungsorganisationen und die Zusammenarbeit mit Unternehmen

Sowohl die NSA als auch der britische Geheimdienst arbeiteten laut Snowden Unterlagen mit mehreren Unternehmen zusammen, um an die Daten sowohl von Mitarbeitern als auch von Nutzern zu kommen. Folgend sollen einige Beispiele genannt werden.
Die British Telecom oder auch Vodafone Cable sollen gegen Bezahlung Computerprogramme entwickelt haben, die es dem Geheimdienst leichter gemacht hat, an ihre Daten zu kommen[49].
2013 wurde bekannt, das Level 3 - eine Firma in Deutschland die mehrere große Rechenzentren und Internetknoten betrieb - den Geheimdiensten die Überwachung des größten Internetknotens in Frankfurt am Main ermöglicht hat.[50]
Die Geheimdienste zahlten mehreren Unternehmen bis zu 278 Millionen US-Dollar, um an deren Daten zu gelangen. Bekannt wurde ebenfalls, dass mindestens 7 große Telekomfirmen mit der NSA und anderen Geheimdiensten zusammen gearbeitet haben, sodass diese die Telekommunikationsdaten und Netzwerkdaten abfangen konnten.[51]
Hier zeigt sich also, eine besonders sensitive Form der Kooperation zwischen dem Staat und der Privatwirtschaft, um auf diese Weise Lücken der Überwachung zu schließen, die sich ansonsten ergeben würden. Der Umfang einer solchen Zusammenarbeit wirft im Einzelnen heikle Fragen auf.

Unternehmen	**Branche**
British Telecom	Telekommunikationsbetreiber
Global Crossing	Netzbetreiber
Interoute	Netzbetreiber
Level 3	Netzbetreiber
Verizon	Telekommunikationsbetreiber
Vital	Netzbetreiber
Vodafone Cable	Telekommunikationsbetreiber

Tabelle 1: Unternehmen, die mit Geheimdiensten zusammen gearbeitet haben

[49] https://www.heise.de/newsticker/meldung/Ueberwachungsaffaere-NSA-zahlt-Hunderte-Millionen-Dollar-an-Provider-1945984.html
[50] http://www.webcitation.org/6JFsTheGR
[51] http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthuellt-namen-der-spaehenden-telekomfirmen-1.1736791

7. Abwägung zwischen Überwachung und Freiheit

Die obige Beschreibung der Überwachung des einzelnen durch den Staat zeigt auf, wie wichtig die Überwachung ist, aber auch welche Gefahren sie für den Bestand der freiheitlichen Gesellschaft mit sich bringt. Eine Gesellschaft ohne jede Überwachung ist unter den heutigen Umständen nicht denkbar, aber eine unbegrenzte Fortentwicklung moderner Formen der Überwachung erscheint auch nicht akzeptabel. Die entscheidende Frage ist, welche Arten der Überwachung erlaubt sind und wo die Grenzen verlaufen. Im letzten Kapitel dieser Literaturanalyse soll festgestellt werden, welche Argumente für und gegen die Überwachung vorhanden sind. Zunächst wird für die Überwachung gesprochen und im Anschluss daran für die Freiheit.

7.1. Argumente für die Überwachung

Das stärkste Argument das hierbei genannt werden kann, ist die größere Chance auf Sicherheit. Dies bedeutet, das kriminelle Geschäfte - egal ob Bombenherstellung, Kinderpornografie oder ein Terroranschlag - schneller gefunden und im Keim erstickt werden können.[52]

Vergegenwärtigt man sich, die Bedrohung der Sicherheit durch Terroristen, organisierte Kriminalität, die Verbreitung von Massenvernichtungsmittel, aber auch Verbrechen wie Geldwäsche so wird deutlich, dass der Staat zur Sicherheit seiner Bürger nicht ohne die Beschaffung von Informationen arbeiten kann, die öffentlich nicht zugänglich sind.

Wer nichts zu verbergen hat, hat auch nichts zu befürchten. Dieses Argument nennt sich in Fachkreisen „Nothing-to-Hide“. Das bedeutet, wenn Bürger rechtsschaffend sind und nichts zu verbergen haben, brauchen sich diese auch keine Gedanken über potenzielle Überwachung machen.[53]

[52] https://www.wen-waehlen.de/btw09/kandidaten/begruendung_1056.html
[53] http://www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639

Das Bundesverfassungsgericht fällte 1983 das Volkszählungsurteil. Darin kam zum ersten Mal das Recht auf Selbstbestimmung im Zusammenhang mit der Volkszählung vor. Eines der Argumente für die Überwachung war, dass die Metadaten die gespeichert werden, harmlos seien und keine personenbezogenen Daten beinhalten würden.[54]

Ein weiteres Argument für die Überwachung kann die Großdatensammlung sein. Hierbei werden alle Daten von Nutzern der sozialen Netzwerke auf Vorrat gespeichert und können später ausgewertet werden. Natürlich sind gerade solche großangelegte Datenbanken in der Öffentlichkeit heute umstritten, weil sie dem Staat ein umfassendes, unbegrenztes Profil eines jeden einzelnen Bürgers ermöglichen können, ohne das der Bürger davon spezielle Kenntnisse hätte. Dabei ist zu erwähnen, dass die Nutzer ihre Posts und Informationen freiwillig auf den Netzwerken posten und somit kein Eingriff in die Privatsphäre stattfindet, wenn die Daten gespeichert werden.[55]

Das Volkszählungsurteil beschreibt die Datensammlung als eine Aufklärung über Wirtschaft und Infrastruktur. Die Daten können für spezielle Ziele genutzt werden, um Städte oder Regierungsprogramme zu verbessern. Die räumliche Verteilung und die Zusammensetzung der Menschen in demographische und soziale Merkmale seien Grundlagen für gesellschaftspolitische und wirtschaftspolitische Entscheidungen des Bundes, der Länder und Gemeinden.[56]

Hier zeigt sich also, dass der Staat zur Durchführung seiner unbestrittenen Aufgaben immer wieder auf genaue Daten angewiesen ist, die ihm sachgerechte Entscheidungen ermöglichen.

7.2. Argumente für die Freiheit und die Beschränkung der Überwachung

In vorangegangen Kapiteln kamen Würde und Freiheit des Menschen zur Sprache. Diese beiden Artikel aus dem Grundgesetz bilden die Basis für eine Demokratie. Überwachung ist ein klarer Verstoß gegen die Grundrechte. Eine Demokratie ist mit der Überwachung nicht vereinbar. Die freie Entfaltung der Persönlichkeit ist ebenfalls unumgänglich für ein demokratisches Land.

[54] https://openjur.de/u/268440.print
[55] http://www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639
[56] https://openjur.de/u/268440.print

Wir leben in einer Informations- und Kommunikationsgesellschaft. Das bedeutet die Verbreitung von Informationen findet auf modernste Art und Weise statt. Bei der Speicherung von Telefondaten zum Beispiel ohne jeglichen Anfangsverdacht ist diese Art der Gesellschaft nicht mit der Überwachung vereinbar.[57]

Der Eingriff von Geheimdiensten in Computer und dem Internetverkehr kann sich immer wieder als inakzeptabler Verstoß gegen die Privatsphäre darstellen, hier werden die Grenzen überschritten. Jeder PC ist ein privater Lebensraum. Und dieser Raum darf nicht ohne Grund überschritten werden, da sonst der sogenannte „Chilling Effect" einsetzt. Ein Staat, der kein Vertrauen in seine Bürger hat, wird auf Dauer nicht überlebensfähig sein.[58]

Es muss dabei bleiben, wie im Volkszählungsurteil festgelegt, dass im Grundsatz der Einzelne über seine Daten Kenntnis hat und darüber verfügen kann, und zwar alleine. Wichtig ist, dass die Arten und die Ziele der Überwachung und insbesondere auch deren Grenzen vom Staat genau festgelegt werden, und nicht im Einzelnen von den Überwachungsbehörden beliebig bestimmt werden können.[59]

Ein weiteres Recht in Deutschland beschreibt das Recht auf Unschuldsvermutung. Dies bedeutet, dass jeder als unschuldig gilt, bevor seine Schuld nicht durch ein rechtskräftiges, gerichtliches Verfahren bewiesen wurde. Durch die unbegrenzte Vorratsdatenspeicherung wird gegen das Recht verstoßen, das annimmt, die überwachten Personen seien schuldig.[60]

Ein weiteres Argument für die Freiheit ist die Meinungsfreiheit. Wenn Menschen denken, sie würden überwacht werden, ändern sie aus Angst ihr Verhalten und überlegen ganz genau, welche Meinung sie zu wem, wann und wo sagen. Der „Chilling Effect" wird hier ersichtlich.

Das letzte Argument ist ebenfalls wichtig für die Freiheit. Die Demokratie beruht auf der freien Meinungsbildung der Öffentlichkeit, „auf dem Marktplatz der Ideen", nur der freie Austausch erlaubt die demokratisch fundierte Willensbildung. Hierzu gehört auch, das jeder Arzt, jeder Rechtsanwalt jeder Pfarrer und jeder Psychologe keine Auskunft über seine Patienten geben darf. Die Schweigepflicht tritt hierbei in Kraft. Berufspflichten verbieten also Überwachung. Denn seit einigen Jahren werden Patientenakten immer mehr elektronisch angefertigt.

[57] http://www.fluter.de/freiheit-oder-sicherheit
[58] http://www.fluter.de/freiheit-oder-sicherheit
[59] https://openjur.de/u/268440.print
[60] http://gesetze-und-rechte.de/tag/unschuldsvermutung/

Wenn es also keine Probleme darstellt, Internetknoten anzuzapfen, dann wird es für Geheimdienste ebenfalls von geringer Problematik sein, Patientendaten oder Klientendaten zu überprüfen. Es bedarf einer gerichtlichen Verfügung diese Akten einsehen zu dürfen.

7.3. Fazit

Zusammengefasst lässt sich sagen, dass die staatliche Überwachung einerseits immer durch den Punkt „Sicherheitsgewährleistung“ gerechtfertigt werden kann, andererseits aber auch die Freiheit des Menschen durch Privatsphäre, Meinungsfreiheit und die Entfaltung der freien Persönlichkeit vertretbar ist. Es lässt sich streiten, wer unter welchen Umständen überwacht werden darf und wer nicht. Die Gesellschaft wird dazu im Lichte immer wieder neuer Situationen ihre Maßstäbe entwickeln. Fakt ist jedoch, dass die Überwachung dort erfolgen muss, wo die Sicherheit gefährdet ist. In Deutschland ist es erlaubt, bei hinreichendem Verdacht, die Daten von Personen auszuspähen.

Es stellt sich jedoch die Frage, ob die Massenüberwachung in den USA besser gerechtfertigt werden kann, als die Überwachung in Deutschland. Die Argumente sind also ausgeglichen und es kommt auf den einzelnen an, wie er mit der Überwachung umgeht und sein Leben entsprechend einrichtet. Eine endgültige Antwort auf die gestellten Fragen wird sich nicht finden lassen. Die Freiheit des Bürgers und seine Sicherheit müssen je nach den Arten der Bedrohung immer wieder neu überdacht und abgewogen werden.

8. Beschreibung der Forschungsmethode

In diesem Kapitel soll verdeutlicht werden, welche Forschungsmethode wieso gewählt wurde. Die Grundlagen der Experteninterviews, der Umfragen und der Aufbau des Fragebogens fallen ebenfalls in dieses Kapitel.

Betrachtet man die Vielzahl der möglichen Forschungsmethoden in einer Bachelor Arbeit wird klar, dass die richtige Methode gut überlegt sein muss. Vor allem ist es wichtig, die richtige Begründung zu geben. Im Folgenden werden Experteninterviews und Umfragen genauer erläutert. Am Schluss wird die Forschungsmethode dieser Bachelor Arbeit verdeutlicht.

Genau wie bei den Experteninterviews ist die Fragestellung bei einer Umfrage sehr wichtig. Bei der Umfrage sollte ein Fragebogen erstellt werden, bei dem Multiple-Choice Antworten, Bewertungsantworten und Antworten auf offene Fragen möglich sind. Hierbei ist eine klare und einfache Sprache von Vorteil. Widersprüchliche Fragen sollte vermieden. [61] Außerdem sollte der Fragebogen klar strukturiert sein. In die Einleitung kommen allgemeine Aspekte wie Vorstellung des Passanten und des Forschenden. Des Weiteren muss vermerkt werden, wie viel Zeit die Umfrage in Anspruch nimmt und dass die Daten vertraulich behandelt werden. Um eine repräsentative Umfrage machen zu können ist es wichtig, die Grundgesamtheit zu definieren. Im Rahmen einer Bachelor Arbeit ist es selten möglich, ganz Deutschland im Alter zwischen 18 und 40 zu befragen. Diese Generation ist mit der digitalen Kultur aufgewachsen und wird als „digital natives“ bezeichnet, wie in Kapitel 10 beschrieben wird. Außerdem ist wichtig zu verstehen, dass die so umgrenzte Gruppe eingegrenzt werden muss. So könnte zum Beispiel die Fragestellung in eng gepasster Weise lauten: “Beeinflusst die staatliche Überwachung der Social-Media-Kommunikation das Verhalten der jungen Nutzer auf der Königsstraße in Stuttgart.

Sobald die Gruppe festgelegt und der Fragebogen erstellt ist, erfolgt die Umfrage und danach die Auswertung

Bei den Experteninterviews kommt es auf die richtigen Fragen an. Dies bedeutet, das Fragen bei denen der Experte nur mit Ja oder Nein antworten kann, vermieden werden sollten.[62]

Die Auswahl der Experten ist ebenfalls wichtig für die Repräsentativität bei der späteren Beantwortung der Forschungsfrage. Wichtig ist zu wissen, dass ein Experte übermäßiges Wissen in einem bestimmten Fachgebiet besitzt. Experten können also Dozenten, Autoren, in der Branche arbeitende, Politiker, Polizisten oder Journalisten sein.

[61] https://karrierebibel.de/bachelorarbeit-umfrage/
[62] https://www.scribbr.de/tipps/experteninterview-bachelorarbeit/

Ebenfalls sind Rechtsanwälte oder Ärzte mögliche Experten. Das Interview sollte semi-strukturiert sein. Dies bedeutet, der Experte kann frei reden, das Interview hat jedoch ein klares Konzept mit geschlossenen Fragen.

Die Forschungsmethode die von Sarah Schmidbauer für diese Arbeit gewählt wurde, mag auf den ersten Blick aus der Norm fallen, wurde aber trotzdem bewusst gewählt. Zunächst ist wichtig zu erwähnen, dass die unten folgenden Forschungsergebnisse keinesfalls repräsentativ sind. Sie sollen lediglich zeigen, wie ein Ergebnis bei einer groß angelegten Forschung mit den festgelegten Maßstäben aussehen könnte. Diese Forschungsarbeit ist Explorativ. Aufgrund dessen werden die Ergebnisse mit „möglicherweise“, „könnte aussehen“ oder „ergäbe“ betitelt. Die Fragestellung lässt viele Möglichkeiten zu. Jedoch entschied sich die Verfasserin, eine neue Art der Forschungsmethode zu wählen. Diese inkludiert die Umfrage von Passanten, die Experteninterviews auf Basis eines Fragebogens und dem Vergleich der beiden Gruppen. Damit die Methode zu sinnvollen Aussagen führt, müssen beide Gruppen mit denselben Fragen konfrontiert werden. Aufgrund dessen wurde ein Fragebogen erstellt, der auf Multiple-Choice Basis beantwortet werden kann. In den folgenden Kapiteln wird sowohl auf die Passantengruppe eingegangen als auch auf die Experten. Die explorative Umfrage beschränkt sich bei den Passanten auf die Digital Natives entlang der Königsstraße und die Experten wurden sorgfältig von der Verfasserin ausgewählt und jeweils per Mail kontaktiert. Die Experten wurden je nach deren unterschiedlichen Sichtweisen und Perspektiven ausgewählt. Digital Natives wird in Kapitel 10 genauer erläutert.

8.1. Aufbau des Fragebogens

Der erstellte Fragebogen soll aufzeigen, wie eine mögliche groß angelegte Forschung aussehen könnte. Zu den wichtigsten Punkten einer gelungenen Umfrage zählen Fragebogen, die Fragestellung allgemein, die Auswahl der Befragten und die spätere, richtige Auswertung der Antworten. In diesem Kapitel wird der Fragebogen genauer erläutert. Unter anderem wird der Aufbau des Bogens erläutert und die Fragen genauer beleuchtet.

Der Fragebogen ist in vier Sachthemen, mit insgesamt 19 Fragen, gegliedert. Das erste Sachthema ist die persönliche Einstellung und Wissen zum Thema staatliche Überwachung der Social-Media-Kommunikation. Die gestellten Fragen werden im nächsten Unterkapitel genauer erläutert. Die persönliche Einstellung ist ein guter Einstieg um aus den späteren Fragen die unbewussten Folgen der Social-Media Überwachung abzuleiten.

Die gestellten Fragen wurden so gewählt, um zu berücksichtigen das grundsätzlich zwei unterschiedliche Standpunkte denkbar sind: Die erste Gruppe verzichtet ungern auf ihre Privatsphäre und ihre Meinungsfreiheit, die zweite Gruppe schenkt der Überwachung allgemein keine besondere Aufmerksamkeit. Das nächste Sachthema be-

schäftigt sich mit der persönlichen Einstellung zum Thema Datenschutz und Datensicherheit. Hier war methodisch zu berücksichtigen, dass wiederum grundsätzlich unterschiedliche Standpunkte bewusst oder unbewusst in Frage kamen. In Frage 11 zum Beispiel geht es darum, ob und wie sich die Passanten in den sozialen Netzwerken vor der staatlichen Überwachung schützen. Hier ergaben sich im ganzen fünf Möglichkeiten, die im folgenden Kapitel näher erläutert sind. Diese Überlegung ist auf explorativer Basis und kann nicht in Anspruch nehmen, ein endgültiges Forschungsergebnis zu beschreiben.

Das dritte Thema des Fragebogens beschäftigt sich mit dem Selbstbestimmungsrecht. Wie bereits in Kapitel vier erläutert, ist das Selbstbestimmungsrecht im Grundgesetz nicht ausdrücklich verankert. Die Frage die hier gestellt werden muss ist zum einen, ob dieses Recht dem einzelnen wichtig ist und ob es in der Wirklichkeit umgesetzt wird. Hier kommt die Arbeit zum Ergebnis, das bei einer großen Forschung die Beantwortung der Frage davon abhängig war, wie die vorigen Fragen beantwortet wurden. Die Ergebnisse von Sarah Schmidbauer finden sich unten in Kapitel 12. Jedoch ist auch wiederum zu berücksichtigen, dass diese Studie nur aufzeigen soll, wie das Ergebnis einer repräsentativen Studie aussehen könnte.

Das letzte Sachthema beschäftigt sich mit den Folgen der Überwachung. Hier ist wichtig zu erwähnen, dass die Befragten direkt auf die Folgen angesprochen werden. Durch die Subjektivität der Antworten ist es ebenfalls zu empfehlen, die vorangegangenen Antworten zu analysieren und mit einzubeziehen.

Der erstellte Fragebogen ist logisch aufgebaut, da er alle Teile der Hypothese abdeckt. Staatliche Überwachung im Allgemeinen, Datenschutz und Datensicherheit (inklusive Selbstbestimmungsrecht) und die möglichen Folgen der Überwachung auf den Einzelnen.

8.2. Die Fragen im Detail

In diesem Kapitel werden die genauen Fragen erläutert und begründet. Bei den Fragestellungen ist zu beachten, dass sie einfach und detailliert gestellt werden. Im Gegensatz zu einem Interview sollte darauf geachtet werden, dass die Fragen nicht offen gestellt werden, sondern kurz und strukturiert sind. Die Verfasserin der Arbeit befragte zunächst 30 Passanten um zu sehen, welche Antworten gegeben wurden. Daraufhin wurde die Fragestellung ausgewählt und ein entsprechender Fragebogen erstellt. In vieler Hinsicht ist festzustellen, dass es darum geht, die grundsätzliche Einstellung der Befragten aus einer Vielzahl von Antworten abzuleiten, wobei Überschneidungen notwendig auftreten und wegen des jeweiligen Zusammenhangs aus bewusst in Kauf genommen werden.

Der erste Fragenblock (Sachthema „persönliche Einstellung und Wissen zum Thema staatliche Überwachung der Social Media Kommunikation) besteht aus 12 Fragen. Diese sind entweder nur mit „Ja“ oder „Nein“ zu beantworten oder aber mit erweiterten Antwortmöglichkeiten.

Die ersten zwei Fragen beziehen sich auf Facebook und WhatsApp. Hier werden die Passanten gefragt, ob sie die beiden sozialen Netzwerke nutzen oder nicht. Somit waren die Antwortmöglichkeiten auf „Ja“ oder „Nein“ begrenzt. Weiter geht es mit der Frage, wie die Meinung zur staatlichen Überwachung der Social-Media-Kommunikation ist. Hier gibt es fünf verschiedene Antwortmöglichkeiten: zu geringes Wissen über die Überwachung, Privatsphäre wird eingeschränkt, gut, da es der Prävention von Vergehen und Verbrechen hilft, es wird ein Grund für die Überwachung benötigt und das Argument „Nothing to Hide“. Die nächsten zwei Fragen beziehen sich auf die Nutzung von Facebook und WhatsApp durch den jeweils befragten. Diese sollen aufzeigen, zu wieviel Prozent die Befragten die Social-Media-Kanäle privat und oder geschäftlich nutzen. Die Antwortmöglichkeiten waren wie folgt: 100%:0% (privat:geschäftlich), 80:20, 70:30, 60:40 und 50:50. Bei der prozentualen Nutzung von Facebook sahen die Antwortmöglichkeiten gleich aus. Die Fragen fünf bis zehn beschäftigen sich direkt mit der Meinung der Passanten zu bestimmten Aussagen der staatlichen Überwachung. Hier geht es also darum, die Einstellung der Befragten konkret im Einzelnen zu erfassen. Fragen sechs und sieben sollen verdeutlichen, was für und was gegen die staatliche Überwachung der Social Media Kanäle sprechen könnte. Bei der Frage „Was spricht für die staatliche Überwachung der Social-Media-Kommunikation“, hatten die Passanten folgende Antwortmöglichkeiten: Prävention bei Vergehen und Verbrechen, „Nothing to Hide“ und kein Argument spricht dafür.

Bei der gegenteiligen Frage („Was spricht gegen die staatliche Überwachung der Social Media Kommunikation“) konnten die Befragten zwischen folgenden Antwortmöglichkeiten wählen: Privatsphäre wird nicht eingehalten, Unschuldsvermutung zählt nicht mehr, Freiheitseinschränkungen finden statt und nichts spricht dagegen.

Die Fragen 8 bis 11 sind reine „ja oder nein“ Fragen. Bei der Frage „Stört Sie auch ein allgemeines Gefühl der Überwachung“ ist wichtig zu erwähnen, dass hier die Antwort von Frage 3 („Wie ist Ihre persönliche Meinung zur staatlichen Überwachung“) verstärkt werden kann. Bei der Auswertung einer groß angelegten Forschung ist es möglich eine Gemeinsamkeit bei der Prozentzahl der Antworten zwischen Frage 3 und 8 zu erkennen. Die darauf folgende Frage lautet: „Würde Sie es auch stören, wenn möglicherweise das Telefon überwacht wird?“. Hier wird auf die mögliche Störung der Privatsphäre eingegangen. Dies könnte in den Ergebnissen einer repräsentativen Studie zu sehen sein.

Frage 10 - „Gehen Sie davon aus, dass unsere Rechtsordnung im ganzen Staat zu viele Möglichkeiten der Informationssammlung über den Einzelnen einräumt“ - spielt unter anderem auf den Zugriff der Vorratsdatenspeicherung verschiedener Firmen (Amazon, Facebook, Google) an.

Hier sind erneut nur „ja“ oder „nein“ als Antwort möglich. Die letzte Frage im „Ja oder Nein“ Block ist folgende: „Glauben Sie, dass staatliche Überwachung bei der Prävention von Verbrechen und Vergehen hilft?“ Bei der Auswertung der explorativen Studie und bei der Auswertung einer groß angelegten Forschung ist eine mögliche Verbindung der Antworten von Frage 3 und 10 zu sehen.

Die letzte Frage des ersten Sachthemas lautet wie folgt: „Wenn es um die Abwägung von Freiheit des einzelnen und die verstärkte Überwachung geht, welchen Schwerpunkt würden Sie dann setzen?“. Hier geht es also um die grundsätzliche Bewertung der Privatfreiheit und der Sicherheit in ihrem gegenseitigen Gewicht. Die Antwortmöglichkeiten waren: verstärkte Überwachung, Freiheit oder 50:50.

Das zweite Fachthema beinhaltet drei Fragen. Hierbei gab es verschiedene Antwortmöglichkeiten. Frage 13 beschäftigt sich mit der persönlichen Meinung zum Thema Datenschutz. Die darauf folgende Frage behandelt das „wieso“. Die Fragen lauten: „Wie schützen Sie sich in den sozialen Netzwerken vor der staatlichen Überwachung“ und „ wieso wollen Sie sich schützen oder nicht schützen“. Diese Fragen zielen darauf ab, die Einstellung der Befragten zur Notwendigkeit des Schutzes der Privatsphäre bei der Nutzung von Facebook und WhatsApp zu analysieren. Die Antwortmöglichkeiten bei Frage 13 waren: keine persönlichen Daten, Verschlüsselungssoftware, Fake-Name und gar kein Schutz. Die nächste Frage („wieso wollen Sie sich schützen oder nicht schützen“) konnte mit den Antworten „schützen wegen Privatsphäre“, „schützen aufgrund der Meinungsfreiheit“, „nicht schützen, wegen des „Nothing to Hide“ Argument und „nicht schützen, aufgrund der eigenen unwichtigen Daten“.

Das dritte Sachthema Selbstbestimmungsrecht umfasst nur zwei Fragen: „glauben sie dass es wichtig ist für Sie, dass ausschließlich Sie selbst, darüber bestimmen, welche Daten der Staat über Sie sammelt und wie der Staat diese Daten verwendet?“ und „Glauben Sie das es in der Wirklichkeit umgesetzt wird?“. Hierbei konnte nur zwischen „ja“ oder „nein“ gewählt werden. Auch dieser Fragenkomplex soll die Einstellung der Befragten im Hinblick auf die Überwachung aus einem anderen Blickwinkel erfassen.

Im letzten Fragenblock wurden die Fragen „Welche Konsequenzen ergeben sich Ihrer Meinung nach schon heute daraus, dass der Staat den Einzelnen in bestimmten Fällen überwacht?“ und „Haben Sie über das Thema Überwachung schon einmal nachgedacht“ behandelt. Bei der Frage nach den Konsequenzen gab es folgende Antwortmöglichkeiten: „Chilling-Effect“, „Einschränkung der Grundrechte“, „Gefährdung der Demokratie“, „Gläserner Bürger“ und „keine Konsequenzen“.

Bei der letzten Frage („Haben Sie über das Thema Überwachung schon einmal nachgedacht“) konnte nur mit „ja“ oder „nein“ geantwortet werden. Dieser letzte Block soll also die Haltung der Befragten zu den Konsequenzen der Überwachung offen legen.

Betrachtet man den ganzen Fragebogen wird deutlich, dass aus allen Fragen nicht nur die reine Antwort als solche genommen werden kann. Auch sind Charaktereigenschaften und Zusammenhänge zwischen Fragen und Antworten erkennbar. So zum Beispiel in Frage 3 („Wie ist Ihre Meinung zur staatlichen Überwachung?“) und Frage 13 („Wie schützen Sie sich in den sozialen Netzwerken vor der staatlichen Überwachung?“). Nähere Informationen folgen in Kapitel 10. Hier ist nochmals daran zu erinnern, das die Antworten zu diesem Fragenkreis thematisch mit einigen oben gestellten Fragen zusammen hängen.

9. Vorstellung der Passanten

Im Folgenden wird eine der wichtigen Fragen geklärt werden. Wie lässt sich die Gruppe der Passanten definieren, die zur Beantwortung der Fragen ausgewählt werden? In welchem Alter sollten diese sein und warum? Was sind Digital Natives? Fragen wie diese sollen in diesem kurzen Kapitel erläutert werden.

Zunächst ist wichtig zu erwähnen, dass diese Studie nur explorativ ist. Dies bedeutet, dass die gewählte Menge der Befragten nicht repräsentativ ist. Es soll lediglich gezeigt werden, wie eine große Forschungsarbeit aussehen könnte. In der explorativen Studie wurden 60 Passanten auf der Königsstraße befragt. Betrachtet man die Studie Deutschlandweit, müssten alle Menschen im „Digital Native“ Alter befragt werden. Hier ist kurz zu beschreiben, was Digital Natives ist und warum nur diese Gruppe für eine Befragung zulässig ist.

Als „Digital Natives“ werden Menschen definiert, die mit den digitalen Medien und den damit verbundenen Technologien aufgewachsen sind. Diese Medien sind unter anderem das Word Wide Web, Laptop, Smartphone und Tablets.[63]Menschen die 1980 geboren sind, können als solche bezeichnet werden. Sie sind im Zeitalter der E-Mails, des Instant Messaging, der Computerspiele und der Smartphones aufgewachsen sind. „Digital Immigrants“ dagegen sind Menschen, die erst im Erwachsenenalter an derartige Technologien heran gebracht wurden. Da die „Digital Natives“ eben mit der Technik aufgewachsen sind, wurden nur Passanten gesucht, die ab 1980 geboren sind. Als dritte Gruppe gibt es die „Digital Illiterates“, die sogenannten digitalen Analphabeten. Diese beherrschen den Umgang mit den digitalen Meiden nicht ansatzweise. Das Mindestalter der Passanten wurde auf 18 Jahre gelegt. Ab diesem Alter sind sie in Deutschland volljährig und können ihre eignen Entscheidungen treffen.

[63] https://de.ryte.com/wiki/Digital_Native

Eine Beschränkung der Umfrage auf die digital natives erscheint deshalb sinnvoll, weil davon auszugehen ist, weil nur diese Gruppe im Stande ist, sich mit dem Thema sinnvoll und bewusst auseinander zu setzen.

Setzt man dieses Konzept in die Tat um und vergrößert die explorative Studie, damit sie in ganz Deutschland vertreten ist, müssten circa 22 Millionen Passanten mit dem vorgegebenen Fragebogen befragt werden, damit später bei der Auswertung ein repräsentatives Ergebnis vorliegt.

9.1. Vorstellung der Experten

In diesem Kapitel sollen die Experten vorgestellt werden. Jedes Experteninterview sollte auf einem stabilen Fundament aus Recherche bestehen. Dies bedeutet, dass die Experten zunächst gründlich ausgesucht werden sollten. Ein Experte definiert sich durch sein vertieftes Wissen auf einem bestimmten Gebiet. Dies bedeutet, dass er beispielsweise in diesem Fall ein Autor von einem Buch sein kann, ein Redakteur der viel über staatliche Überwachung und Medienrecht berichtet und so weiter. Die Experten die Sarah Schmidbauer gewählt hatte, wurden per E-Mail gebeten, an der Umfrage teilzunehmen. Eine E-Mail befindet sich im Anhang. Insgesamt wurden 50 Experten angeschrieben und 30 hatten der Befragung zugestimmt. Im folgenden Abschnitt werden die Arbeitsfelder der Befragten beschrieben. Außerdem werden Zahlen genannt, die zeigen sollen, in welchem Maße die Befragung stattfinden soll, um die Studie auch Deutschlandweit durchzuführen.

Besonders bemerkenswert war, dass alle Experten die angefragt wurden, in der Arbeit nicht mit Namen erwähnt werden wollten. Ihre Begründung war die, dass das Thema zu heikel sei, um offen und mit vollem Namen darüber reden zu können. Dies weißt darauf hin, das auch Experten davon ausgehen, dass es sich um ein Thema handelt, das von der Sache her, aber auch persönlich besonders sensitiv erscheint.

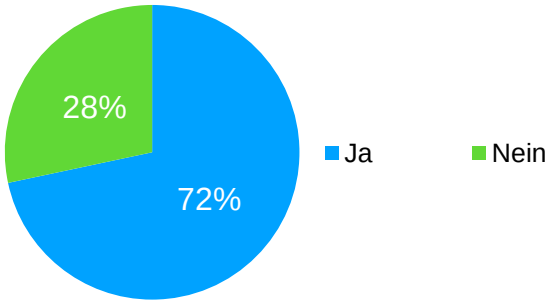
Die Arbeitsfelder der ausgewählten Experten waren sehr vielfältig. Es konnten - wie schon erwähnt - 30 Experten zu der Umfrage bewegt werden. Hierbei wurden 10 Leute aus den Polizeipräsidien in Stuttgart und Heilbronn gefragt. Außerdem wurden 5 Redakteure aus der Kraichgau Stimme und 5 Redakteure aus der Heilbronner Stimme als Experten ausgewählt. Die Parteiprogramme in Stuttgart sind vielseitig. Aufgrund dessen wurden jeweils 2 Abgeordnete aus der CDU, der SPD und der AfD gewählt. In einer großen Forschung könnte hier, bei genügend Experten, auch Unterschiede in den Antworten zu erkennen sein. Kleine Unterschiede sind bereits erkennbar. Mehr dazu gibt es in den Ergebnissen. Weiterhin wurden 4 Rechtsanwälte und ein IT-Experte befragt. Bei einer umfassend angelegten Forschung müssten alle Zeitungen in ganz Deutschland, alle Polizeipräsidien, alle Rechtsanwälte im Bereich Medienrecht, als auch alle Abgeordnete der demokratischen Parteien in Deutschland befragt werden.

Wenn davon ausgegangen wird, dass pro große Zeitung circa 40 Mitarbeiter angestellt sind und diese Zahl mit allen Zeitungen in Deutschland verrechnet wird (circa 60 große Zeitungen) kommt man auf eine Zahl von allein 2400 Redakteure. [64]Wenn wie üblich eine repräsentative Umfrage durchgeführt werden sollte, so müsste eine hinreichende repräsentative Gruppe ausgewählt werden.

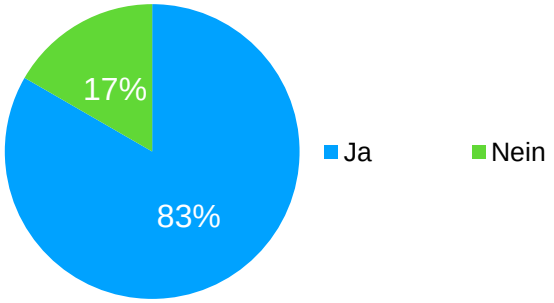
10. Ergebnisse der Passanten

Ergebnisse immer in Gegenwart In diesem Kapitel wird aufgezeigt, welche Ergebnisse die explorative Forschung gebracht hat. Dies dient als Beispiel dafür, wie das Ergebnis einer groß angelegten Studie aussehen könnte.
Wie schon erwähnt, wurden 60 Passanten befragt. Wichtig ist zu erwähnen, dass alle Passanten ihre Meinung zu diesem Thema hatten. Jeder hatte eine passende Antwort parat und zeigte, dass dieses Thema möglicherweise von großem Interesse bei der Bevölkerung sein könnte. Im Folgenden werden die Fragen, die Antwortmöglichkeiten und die Auswertungen aufgezeigt. Ebenfalls wird nach jeder Frage ein Diagramm eingefügt, welches die Auswertung in graphischer Form zeigt.

Frage 1: “Nutzen Sie den Facebook-Messenger?“ Hier waren die Antwortmöglichkeiten auf „Ja“ oder „Nein“ beschränkt. 72% der Passanten antworteten mit „Ja“ und 28% mit „Nein“.

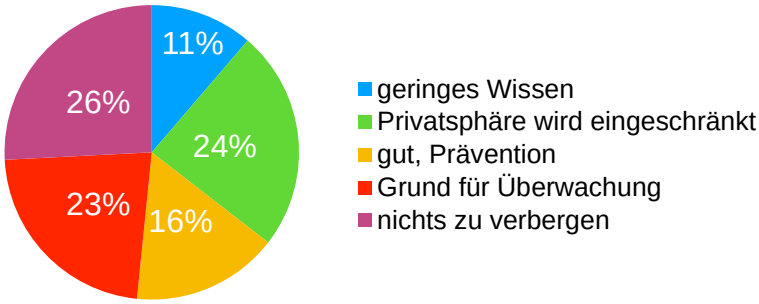


Frage 2: Nutzen Sie WhatsApp? Diese Frage bot dieselben Antwortmöglichkeiten. Hierbei viel jedoch das „Ja“ höher aus. Der prozentuale Anteil lag bei 83% „Ja“ und 17% „Nein“.

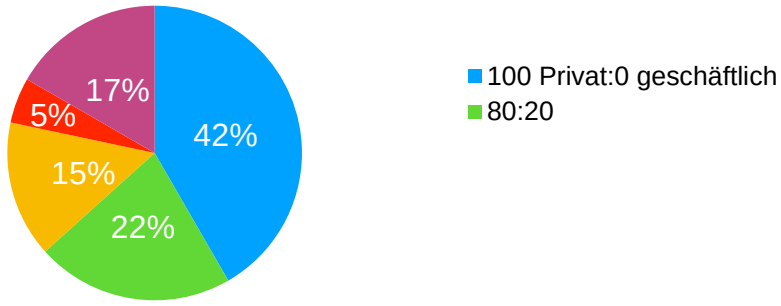


[64] http://www.focus.de/finanzen/geldanlage/top-60_aid_100734.html

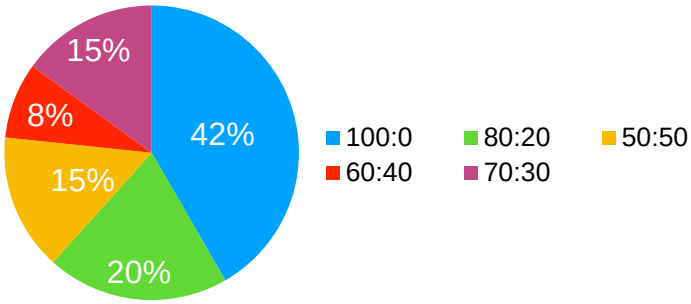
Frage 3: Wie ist Ihre Meinung zur staatlichen Überwachung der Social Media Kommunikation. Die Antwortmöglichkeiten wurden sorgfältig ausgewählt. Diese waren: geringes Wissen über die Überwachung; die Privatsphäre wird eingeschränkt; gut für die Prävention von Vergehen und Verbrechen; es wird ein Grund für die Überwachung benötigt und unwichtig, da der Passant nichts zu verbergen hat (hier also das Argument „Nothing to Hide“). Die Antworten vielen hier unterschiedlich aus. Geordnet lag hier das höchste Ergebnis mit 26% bei dem „Nothing to Hide“ Argument.
Danach folgten mit 24% das die Privatsphäre eingeschränkt wird, mit 23% das ein Grund für die Überwachung benötigt wird, mit 16% dass es gut für die Prävention sei und auf dem letzten Platz lag mit 11% das geringe Wissen über die Überwachung. Hier lässt sich ein erstes mögliches Ergebnis heraus lesen. Die Tatsache, das die Passanten nichts zu verbergen haben zeigt auf, das die Überwachung möglicherweise keine Konsequenzen mit sich bringen könnte.



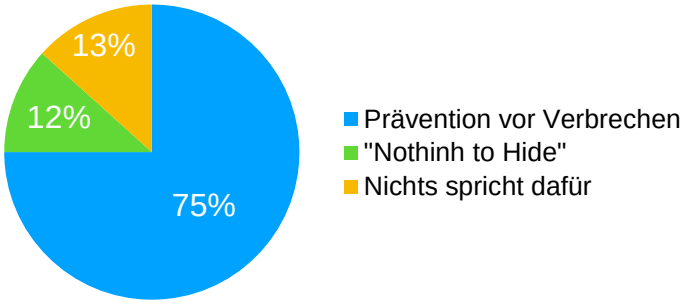
Frage 4: "Nutzen Sie WhatsApp prozentual gesehen mehr für geschäftliche oder private Zwecke?“ Hier gab es folgende Antwortmöglichkeiten: 100:0 (privat:geschäfltich), 80:20, 70:30, 60:40 und 50:50. 42% (und somit die meisten) antworteten damit, dass sie WhatsApp ausschließlich für private Zwecke nutzen würden. Die Begründung war immer, das geschäftliches (sofern ein Geschäft vorhanden) immer in sichereren Netzwerken geklärt werden sollte. Als Beispiel wurde E-Mail und Xing genannt. 80:20 liegt mit 22% auf Platz zwei. Darauf folgen 70:30 mit 17%, 50:50 mit 15% und 60:40 mit 5%. Klar wird hier jedoch, dass das Thema Überwachung möglicherweise im geschäftlichen Bereich (aufgrund sensibler Daten) einen höheren Stellenwert besitzt.



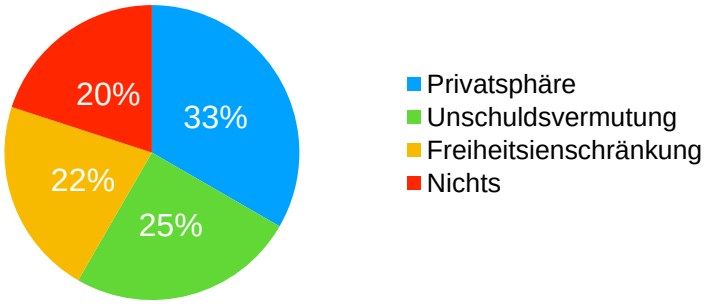
Frage 5: „Nutzen Sie den Facebook-Messnger?“. Hierbei gab es die selben Antwortmöglichkeiten wie in der vorherigen Frage. Allgemein viel das Ergebnis ähnlich wie in Frage 4 aus. Lediglich drei Antworten unterscheiden sich durch 2-3%. Daraus lässt sich schließen, dass WhatsApp und Facebook auf der gleichen Ebene der prozentualen Nutzung sein könnten.



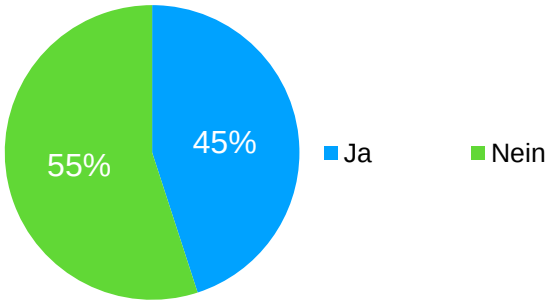
Frage 6: „Was spricht für die staatliche Überwachung der Social Media Kommunikation?“ Die Antwortmöglichkeiten waren hier wie folgt: „Prävention von Verbrechen und Vergehen“; „Nothing to Hide“ und „nichts spricht dafür“. Am meisten wurde mit „Prävention von Verbrechen und Vergehen“ geantwortet. Hierbei lag das Ergebnis bei 75%. Nur 13% antworteten mit „Nichts spricht dafür“. 12% gaben die Antwort, dass sie nichts zu verbergen hätten.



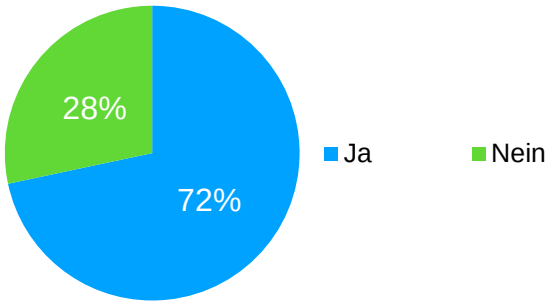
Frage 7: „Was spricht gegen die staatliche Überwachung?“ Als Antwortmöglichkeiten wurden folgende aufgelistet: Privatsphäre wird gestört; die Unschuldsvermutung wird nicht eingehalten; Freiheitseinschränkung und nichts spricht dagegen. 33% fühlten sich in ihrer Privatsphäre gestört, 25% waren der Meinung, dass die Unschuldsvermutung nicht eingehalten werden würde. Während 22% mit der Freiheitseinschränkung antworteten, waren nur 20% der Meinung, dass nichts gegen staatliche Überwachung spräche. Hier zeigt sich also, dass ein beträchtlicher Teil der Befragten die derzeitige Praxis als einschneidend und nicht Akzeptabel ansehen. Dieses Ergebnis ist im Gesamtbild durchaus bemerkenswert.



Frage 8: „Stört Sie auch ein allgemeines Gefühl der Überwachung, selbst wenn Sie dazu nichts im Einzelnen wissen?“. Diese „Ja/Nein“ - Frage soll auf die Realität anspielen. Fakt ist, die Menschen wissen zwar, dass sie überwacht werden, jedoch ist nicht klar, wie, wie oft, wer und mit welcher Begründung überwacht wird. Bei einer großen Studie könnte klar werden, dass viele Passanten ein Gefühl der Überwachung nicht stört, da sie darüber nichts wissen. Bei der explorativen Studie antworteten 55% mit „Nein“ und 45% mit „Ja“.



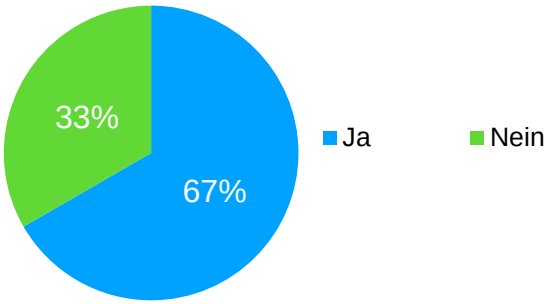
Frage 9: „Würde Sie es auch stören, wenn möglicherweise das Telefon überwacht werden würde?“ Bei dieser Frage könnten bei einer repräsentativen Studie die Prozentzahlen deutlich auseinander liegen. Bei den 60 Passanten wurde zu 72% mit „Ja mich stört die Telefonüberwachung“ geantwortet. Lediglich 28% würde es nicht stören. Bemerkenswert ist also, dass eine hohe Zahl der Befragten einer Telefonüberwachung ablehnend gegenüber stehen.



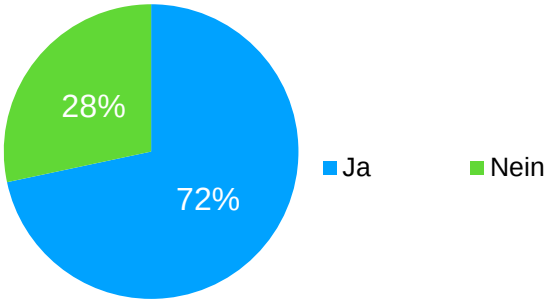
Frage 10: „Gehen Sie davon aus, das unsere Rechtsordnung im ganzen Staat zu viele Möglichkeiten der Informationssammlung über den einzelnen einräumt?“. Diese Frage zielt vor allem auf die Vorratsdatenspeicherung von Facebook oder Amazon ab. Vorratsdatenspeicherungen sind personenbezogene Daten, die für öffentliche Dienste zugänglich sind, jedoch im Moment keinen Nutzen haben. Die Telefondaten dürfen maximal zehn Wochen gespeichert werden, umfassen jedoch was, wann, wer und mit wem gesprochen hat[65].
Es stellt sich also hierbei die Frage, ob die Vorratsdatenspeicherung über das Verhalten von Privatpersonen durch den Staat zulässig ist oder nicht**.** Das Bundesverfassungsgericht hat dazu wie folgt entschieden: Laut dem Urteil von 2017 müssen zukünftig unter anderem Telekommunikationsanbieter die Daten ihrer Kunden speichern. Hierbei gab es großen Gegenwind, jedoch wurde an dem Urteil bis Dato nichts geändert.[66]

[65] http://www.sueddeutsche.de/digital/freiheit-versus-sicherheit-was-sie-ueber-die-vorratsdaten-speicherung-wissen-sollten-1.2438333
[66] https://digitalcourage.de/blog/2017/bundesverfassungsgericht-will-vorratsdatenspeicherung-2017-nicht-verhandeln

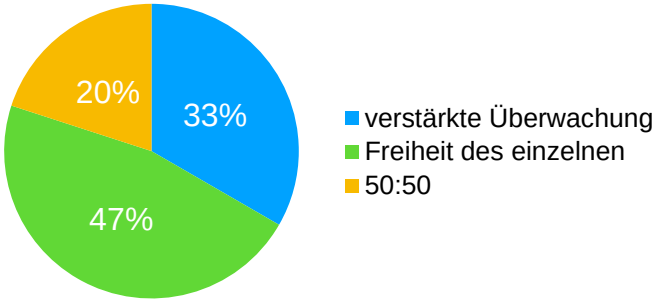
Das Ergebnis bei der explorativen Studie fiel eindeutig aus. 67% bestätigten die Vermutung, dass der Staat zu viele Möglichkeiten der Informationssammlung über den einzelnen einräumt. Lediglich 33% waren nicht dieser Meinung. In einer repräsentativen Forschung könnten diese 67% eventuell noch größer werden.



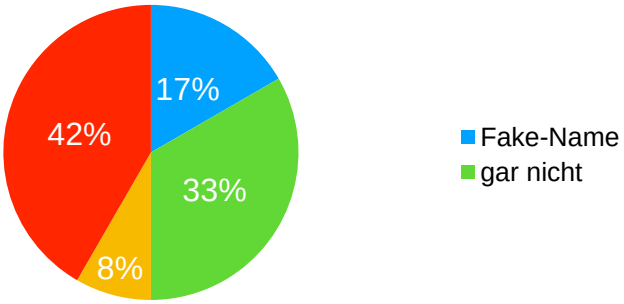
Frage 11: „Glauben Sie, dass staatliche Überwachung bei der Prävention von Verbrechen und Vergehen hilft?“. Hier wurden die selben Prozentzahlen wie in Frage 9 (Telefonüberwachung) ermittelt. 72% bejahten, dass staatliche Überwachung bei der Prävention helfen würde. Vergleichbar ist hier Frage 6 („Was spricht für die staatliche Überwachung?“), bei der ebenfalls mehr als 70% der Meinung waren, die staatliche Überwachung würde bei der Prävention von Verbrechen und Vergehen helfen. 28% der Befragten waren der Meinung, dass die Überwachung nicht der Prävention von Verbrechen dienen würde.



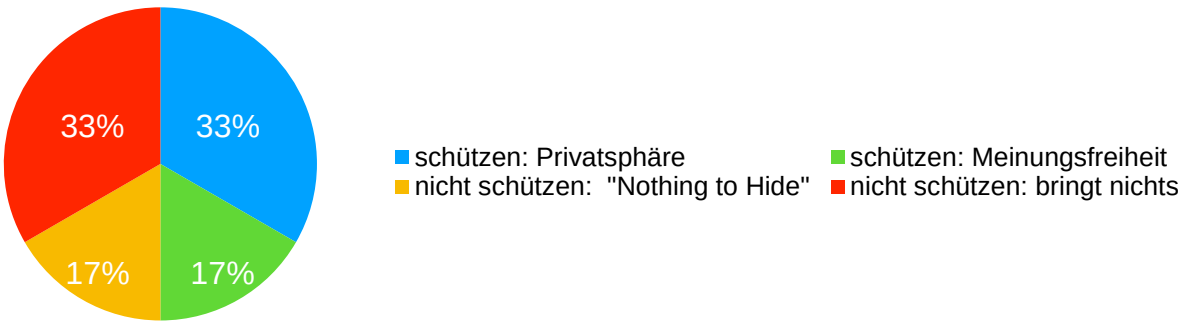
Frage 12: „Wen es um die Abwägung von verstärkter Überwachung und der Freiheit des einzelnen geht, welchen Schwerpunkt würden Sie dann setzen?“. Bei der Literaturanalyse gab es sowohl einige Punkte, die für Freiheit sprachen, als auch Argumente die auf die verstärkte Überwachung angewendet werden konnten. Bei der Frage konnten folgende Antwortmöglichkeiten gewählt werden: Freiheit des einzelnen, verstärkte Überwachung oder 50:50. Bei der Auswertung wurde festgestellt, dass 47% für die Freiheit des einzelnen waren, während 33% für verstärkte Überwachung plädierten. Nur 20% waren für eine Mischung aus beidem. Dieses Ergebnis könnte bei einer groß angelegten Forschung genau so aussehen. Die Antworten sind also zusammenfassend so zu verstehen, dass heute mehr Personen der Auffassung sind, dass künftig in erster Linie die Freiheitsrechte zu betonen sind und weniger die Verstärkung der Sicherheit. Ob dies wirklich gut ist, sollte Inhalt einer anderen Forschungsarbeit sein.



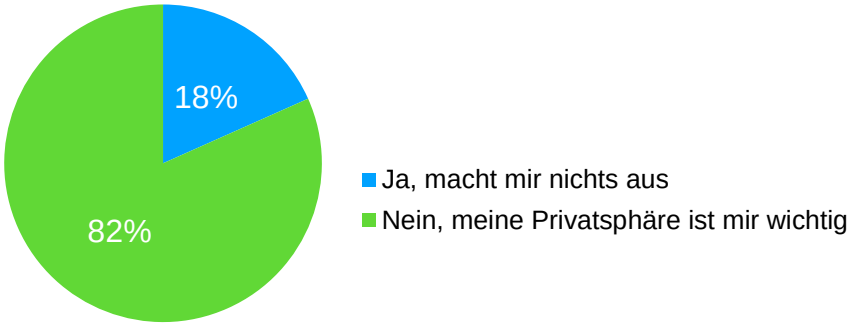
Frage 13: „Wie schützen Sie sich in den sozialen Netzwerken vor der staatlichen Überwachung?“ Diese Frage konnte mit vier Möglichkeiten beantwortet werden: „Fake-Name“, „Software“, „keine persönlichen Daten“ und „gar nicht“. 42% antworteten, dass sie keine persönlichen Daten von sich preisgeben würden, während sich 33% überhaupt nicht schützen. 17% antworteten mit dem Fake-Name und 8% würden sich mit Hilfe einer Verschlüsselungssoftware schützen.
Hier ist bemerkenswert, wie hoch die Zahl der Personen ist, die sich der möglichen Überwachung bewusst sind und deshalb wohl keine persönlichen Daten von sich preisgeben. Hier wäre bei einer umfassenderen Studie noch zu differenzieren, ob insoweit die Bedenken sich in erster Linie gegen die staatliche Überwachung richten oder ob auch die Furcht vor einer Überwachung durch private Personen eine Rolle spielt.



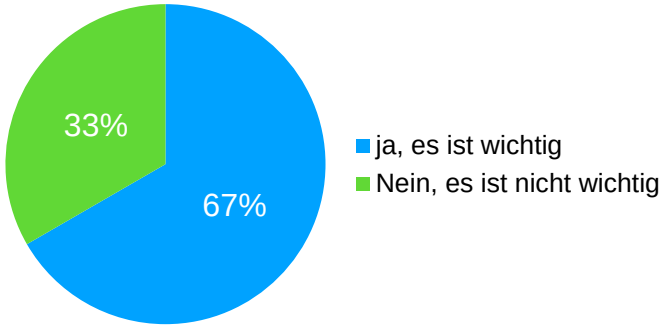
Frage 14: Wieso wollen Sie sich schützen/nicht schützen?“. Hierbei gab es folgende Antwortmöglichkeiten: „schützen, wegen meiner Privatsphäre“, „schützen, aufgrund der Meinungsfreiheit“, „nicht schützen, ich habe nichts zu verbergen“, „nicht schützen, bringt sowieso nichts“. 33% meinten, sie wollen sich schützen, da ihnen die Privatsphäre wichtig sei. Weitere 33% antworteten, dass der Schutz der Daten nichts bringt, da die Regierung so oder so an ihre Daten gelangen könnte. 17% wollten sich schützen, da ihnen die Meinungsfreiheit wichtig wäre. Obwohl dieses Argument etwas paradox klingen mag - wenn man sich schützen möchte, wird dann nicht unmittelbar die Meinungsfreiheit eingeschränkt? Erneut 17% antworteten, dass sie sich nicht schützen würden, da sie nichts zu verbergen hätten.



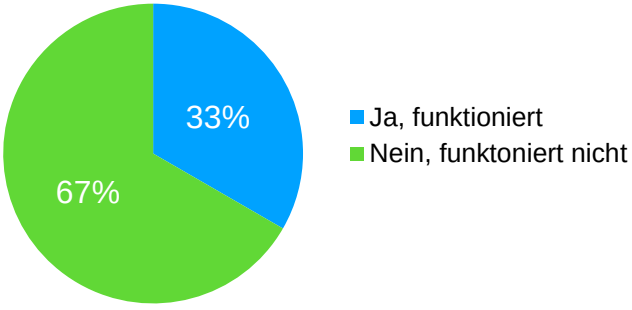
Frage 14: „Geben Sie im Internet persönliche Daten von sich preis?“ Diese Frage soll unterstützend für Frage 13 gelten. Wenn mehr Passanten antworten, dass sie persönliche Daten von sich preis geben, stimmt die Auswertung der 13. Frage nicht. Bei der explorativen Studie hat jedoch alles der vorgesehenen Richtigkeit entsprochen. 82% gaben an, keine persönliche Daten von sich preis zu geben. Lediglich 18% würde es nichts ausmachen, ihre persönlichen Daten in die sozialen Netzwerke zu stellen.



Frage 15: „Glauben Sie dass es wichtig ist für Sie, dass ausschließlich Sie selbst darüber bestimmen, welche Daten der Staat über Sie sammelt und wie der Staat diese Daten verwendet?“. Hier meinten 67% dass es wichtig sei, es jedoch in der Wirklichkeit nicht umsetzbar sei. 33% sagten aus, dass das Selbstbestimmungsrecht nicht wichtig wäre.

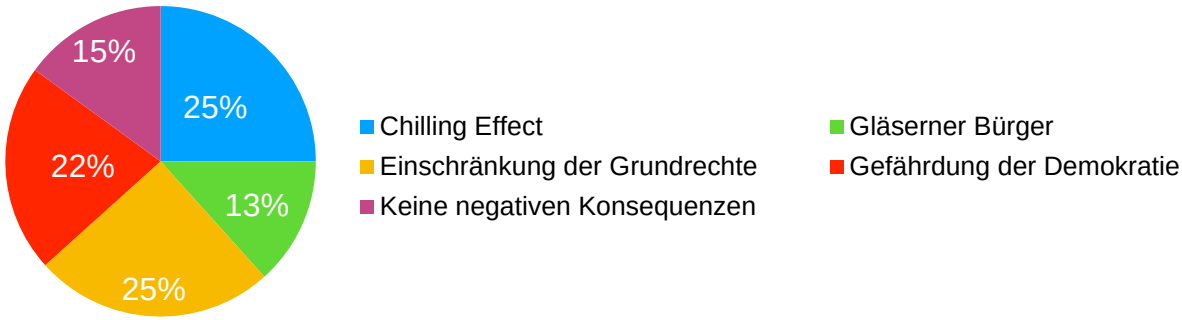


Frage 17: Glauben Sie, dass das Recht in der Wirklichkeit umsetzbar ist? Hier glaubten weitere 33%, dass das informationelle Selbstbestimmungsrecht nicht in der Wirklichkeit umsetzbar ist, aufgrund der (als Beispiel kann hier Amazon genannt werden) AGB’s. Sobald man als Neukunde diese nicht Akzeptiert, wird man nicht weiter geleitet. In den AGB’s steht geschrieben, dass Amazon die persönlichen Daten für bessere Angebote nutzen darf. Bestätigt man also die Bedingungen, legt man automatisch das Recht der Selbstbestimmung in die Hände von Amazon. Dieses Ergebnis lässt sich anhand einer großen repräsentativen Studie überprüfen.

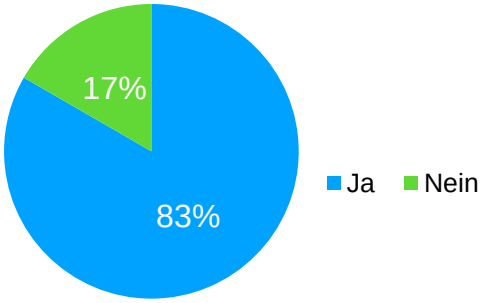


Frage 18: „Welche Konsequenzen ergeben sich nach ihrer Meinung schon heute daraus, das der Staat in bestimmten Fällen den einzelnen Überwacht?“ Die vorletzte Frage zielt direkt auf die möglichen Konsequenzen der staatlichen Überwachung der Social-Media-Kommunikationab. Hierbei gab es folgende Antwortmöglichkeiten: „Chilling-Effect“, „Einschränkung der Grundrechte“, „Gefährdung der Demokratie“, „Gläserner Bürger“ und „keine Konsequenzen“.

25% antworteten damit, dass der „Chilling-Effect“ als mögliche Konsequenz eintreten könnte. Ebenfalls 25% nannten die Einschränkung der Grundrechte als eine mögliche Konsequenz für den einzelnen. 22% der Passanten waren der Meinung, dass die staatliche Überwachung die Demokratie gefährden würde. Hierzu sollte folgendes gesagt werden: Die Demokratie kann nur durch die Bevölkerung definiert werden. Volksentscheidungen wie Wahlen beispielsweise sind das Fundament einer funktionierenden Demokratie. 15% meinten, es gäbe keine Konsequenzen und 13% hatten die Befürchtung, dass die staatliche Überwachung immer mehr gläserne Bürger als Konsequenz mit sich bringt. Hier zeigt sich, dass die Befragten dem Thema Überwachung grundsätzlich eher ablehnend gegenüber stehen. Das Ergebnis zu dieser generellen Haltung deckt sich weitgehend mit dem Ergebnis zu den vorherigen Fragen. Zu bemerken ist, dass diese Antworten rein subjektiver Natur sind. Die unbewussten möglichen Konsequenzen auf den einzelnen lassen sich leichter feststellen, wenn man sich die Frage 13 ebenfalls genauer ansieht. Durch die große Prozentzahl bei der Antwort „ich gebe keine persönlichen Daten von mir preis“ wird klar, dass die Passanten mehr in dem „Chilling-Effect“ sind als sie glauben. Dies wird unter Umständen in einer großen und repräsentativen Umfrage bestätigt werden.



Frage 19: „Hat Sie die Frage der staatlichen Überwachung schon einmal beschäftigt?“ Hier beschränkten sich die Antwortmöglichkeiten auf „ja“ oder „nein“. 83% gaben an, dass sie die staatliche Überwachung schon einmal beschäftigt hat und dieses Thema aktuell ist.

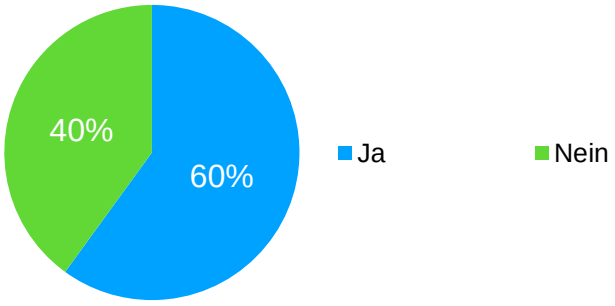


Diese Auswertung der explorativen Studie ist keinesfalls repräsentativ. Sie soll lediglich aufzeigen, in welche Richtung die Ergebnisse einer repräsentativen Studie gehen könnten.

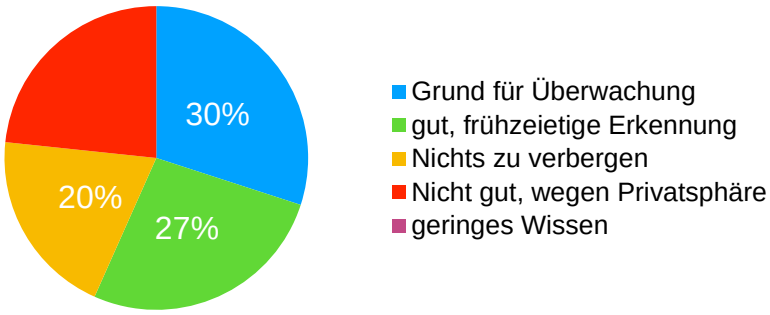
11. Ergebnisse der Experten

In diesem Kapitel richtet sich das Augenmerk auf die Experten. Wie im oberen Kapitel beschrieben, müssten für eine repräsentative Studie circa 140.000 Experten befragt werden. Den Vergleich zwischen Experten und Passanten folgt im 12. Kapitel.

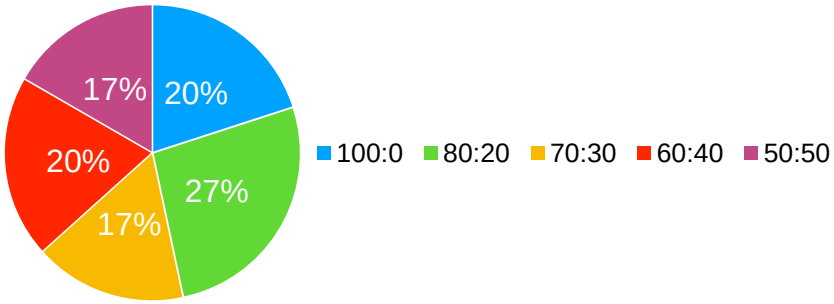
Die erste Frage („Nutzen Sie WhatsApp?“) beantworteten die Experten zu 60% mit „ja“ und 40% mit „nein“. Ebenso die zweite Frage, ob sie den Facebook-Messenger nutzen würden.



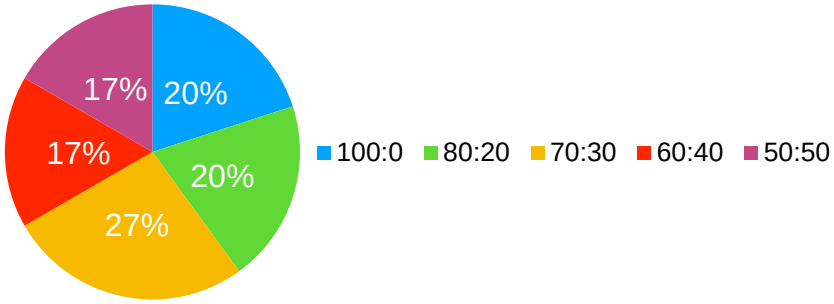
Frage 3 lautete: “Wie ist Ihre Meinung zur staatlichen Überwachung der Social Media Kommunikation?“ Hier antworteten die Experten zu 30% damit, dass es ein Grund für die Überwachung bräuchte, 27% meinten, es sei gut, da eine frühzeitige Erkennung von Vergehen und Verbrechen möglich sei. 23% sahen die Privatsphäre gefährdet und 20% hatten nichts zu verbergen. Bei einer repräsentativen Studie könnte dies in eine ähnliche Richtung gehen. 0% antworteten mit dem Argument, ein zu geringes Wissen über das Thema zu besitzen.



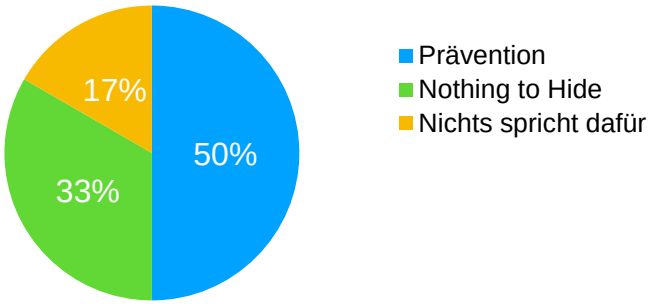
Frage 4: „Nutzen Sie WhatsApp prozentual gesehen mehr für geschäftliche oder private Zwecke?“. Hier gaben 27% an, den Messenger 80% für privates und 20% für geschäftliches zu nutzen. 20% nutzten den Dienst 100% privat. 60% der Experten antworteten, dass sie den Messenger für beides gleich nutzen würden. Politiker beispielsweise nutzen den Facebook-Messenger für die Kommunikation mit Bürgern.



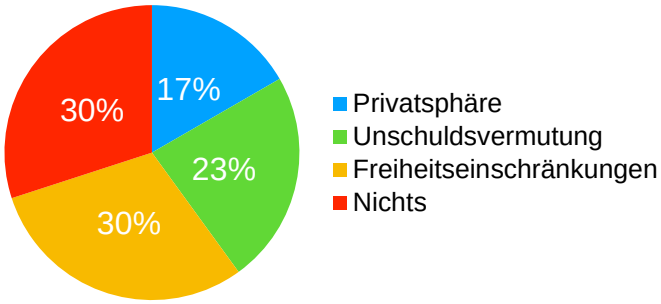
Die Zahlen für den Facebook-Messenger bei der fünften Frage vielen ähnlich aus. Im Gegensatz zum Facebook-Messenger wird WhatsApp bei der 80:20 Nutzung weniger für geschäftliches benutzt. 27% gaben an, WhatsApp mit 70% privatem und 30& geschäftlichem zu nutzen.



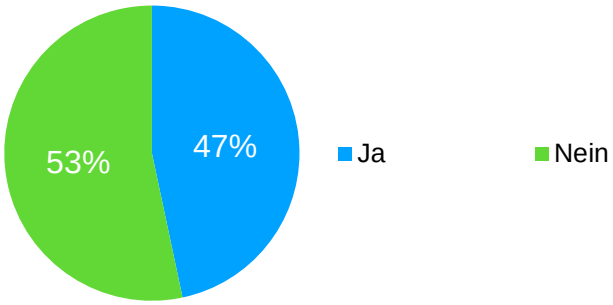
Frage 6: „Was spricht für die staatliche Überwachung der Social Media Kommunikation“ beantworteten die Experten zu 50% mit der Prävention von Verbrechen und Vergehen. 33% meinten, sie hätten nichts zu verbergen, während 17% der staatlichen Überwachung nichts positives abgewinnen konnten.



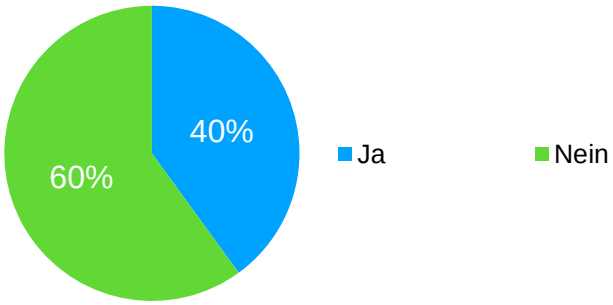
Frage 7: „Was spricht gegen die staatliche Überwachung?“. Bei dieser Frage antworteten 30% der Experten, dass die Freiheit eingeschränkt werden würde. Ebenfalls 30% jedoch meinten, dass nichts gegen die staatliche Überwachung sprechen würde. 23% waren der Meinung, dass die Unschuldsvermutung nicht eingehalten werden würde und 17% brachten den Verstoß gegen die Privatsphäre als Argument an.



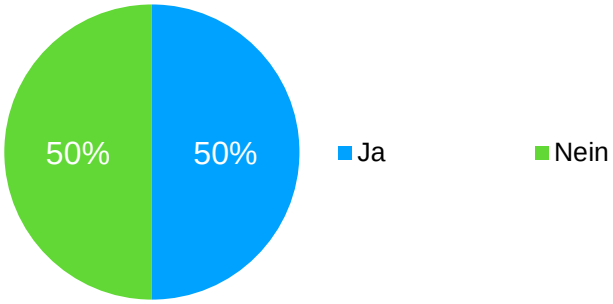
Frage 8: „Stört Sie auch ein allgemeines Gefühl der Überwachung, selbst wenn Sie dazu nichts im einzelnen Wissen?“ Hier antworteten 47% mit „Ja“ und 53% mit „Nein“.



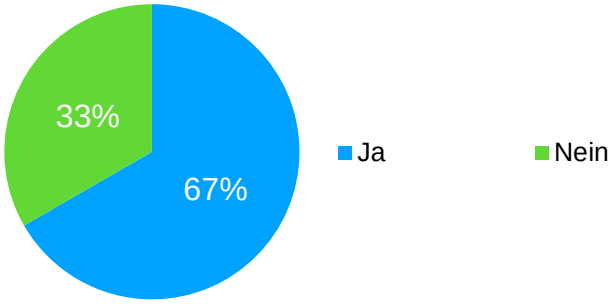
Frage 9: Würde Sie es auch stören, wenn möglicherweise das Telefon überwacht wird? 60% der Experten würde es nicht stören, 40% waren der gegenteiligen Meinung.



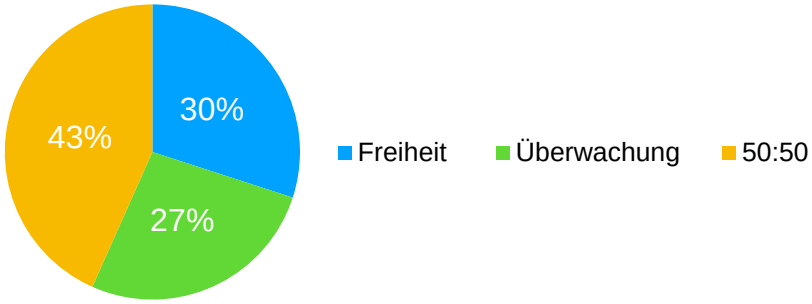
Frage 10 („Gehen Sie davon aus, das unsere Rechtsordnung im ganzen Staat zu viele Möglichkeiten der Informationssammlung über den einzelnen einräumt?“) wurde zu jeweils 50% mit „Ja“ und „Nein“ beantwortet.



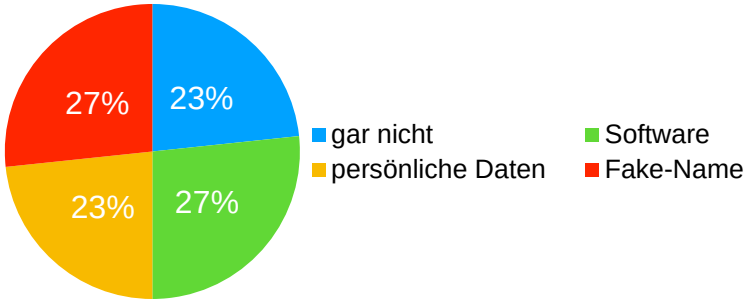
Frage 11: Glauben Sie, dass staatliche Überwachung be der Prävention von Vergehen und Verbrechen hilft?“ Hierbei antworteten 67% der Experten mit „Ja“ und 33% mit „Nein“.



Frage 12: „Wenn es um die Abwägung von Freiheit des einzelnen und die verstärkte Überwachung geht, welchen Schwerpunkt würden Sie dann setzen?“ Die zwölfte Frage wurde zu 43% mit „50:50“ beantwortet. 30% wollten Freiheit und 27% die verstärkte Überwachung.

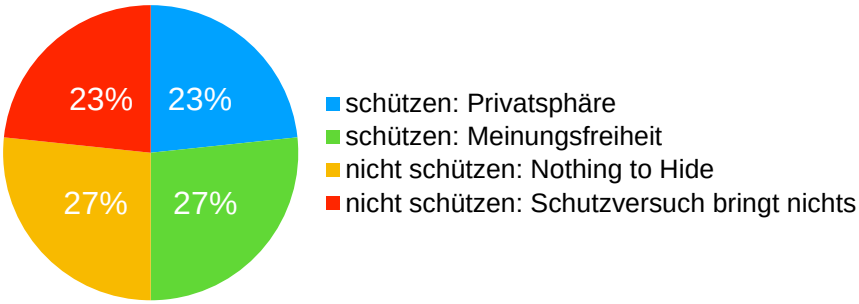


Frage 13: „Wie schützen Sie sich in den sozialen Netzwerken vor der staatlichen Überwachung?“. Hier antworteten 27% mit dem Fake-Namen und weitere 27% mit der Überwachungssoftware. 23% gaben an, keine persönliche Daten von sich preis zu geben, während sich weitere 23% nicht schützen wollen.

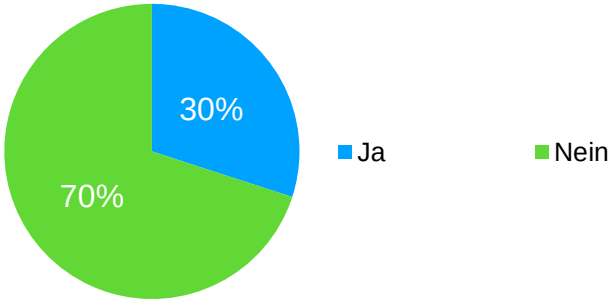


Frage 14: „Wieso wollen Sie sich schützen oder nicht schützen?“ Diese Frage soll die subjektiven Konsequenzen auf den einzelnen Untermauern. Ein Zusammenhang zwischen den Antworten von Frage 14 und der Frage nach den Konsequenzen ist eindeutig vorhanden. Dies könnte in einer repräsentativen Studie noch deutlicher zu sehen sein. 23% der Experten wollten sich wegen der Privatsphäre schützen. 27% aufgrund der Meinungsfreiheit. 23% meinten, der Versuch sich zu schützen würde nichts bringen, während weitere 27% nichts zu verbergen hätten und sich aufgrund dessen nicht schützen müssten.

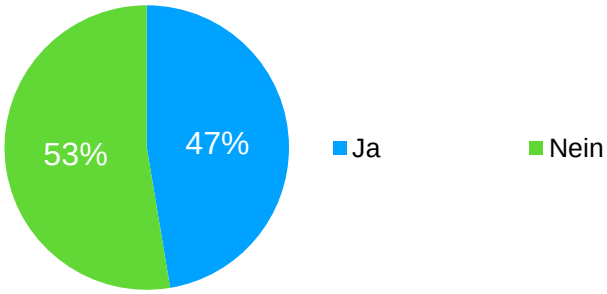
Die 27% die sich, aufgrund der Meinungsfreiheit, schützen wollen, sind deutlich in den Folgen des Chilling-Effects. Sobald man Angst hat, seine Meinung frei zu äußern und sich schützt, wird das Verhalten aufgrund der vorhandenen Angst angepasst. Egal, ob die Meinung geäußert wird oder nur mit Schutz in den sozialen Netzwerken ausgesprochen wird. Diese 27% zeigen die unbewusste Meinung zum Thema Überwachung.



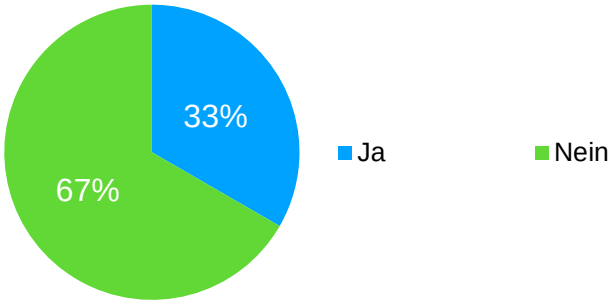
Die Frage, ob Experten ihre persönlichen Daten in den sozialen Netzwerken veröffentlichen würden, zeigte bei den Antworten deutlich, das dem nicht so ist. 70% der Experten gaben an, keine persönlichen Daten von sich auf den sozialen Netzwerken preis zu geben. Nur 30% hatten dagegen nichts einzuwenden. Dies wird in einer großen Studie möglicherweise bestätigt werden.



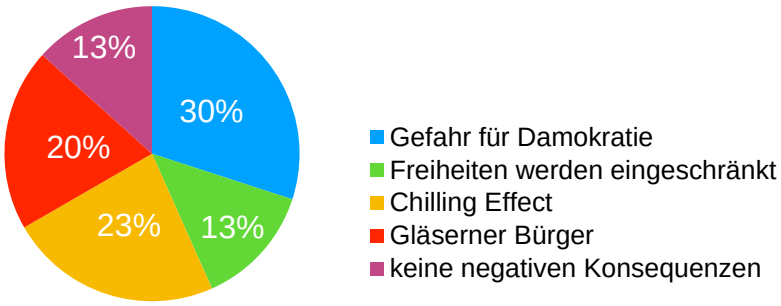
„Glauben Sie das es wichtig ist für Sie, das ausschließlich Sie selbst darüber bestimmen, welche Daten der Staat über Sie sammelt und wie der Staat diese Daten verwendet?“ Frage 16 beschäftigt sich mit dem Selbstbestimmungsrecht. Hier lag die Differenz zwischen „ja“ und „nein“ relativ nah beieinander.53% gaben an, es sei ihnen nicht wichtig, das nur sie über ihre eigenen Daten bestimmen würden. 47% waren der Meinung, dieses Recht sei von enormer Bedeutung für unter anderem eine funktionierende Demokratie.



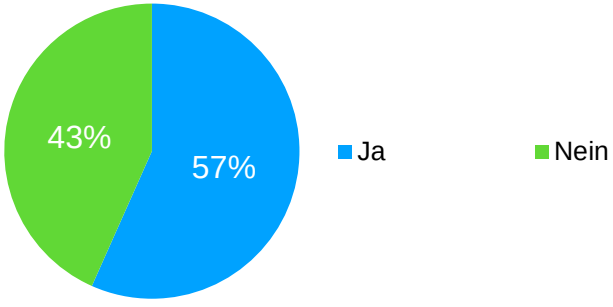
67% der Experten waren der Meinung, dass das Selbstbestimmungsrecht nicht in der Wirklichkeit umsetzbar wäre, während 33% vom Gegenteil überzeugt waren.



Frage 18 lautet folgendermaßen: “Welche Konsequenzen ergeben sich Ihrer Meinung schon heute daraus, das der Staat in bestimmten Fällen den einzelnen überwacht?“ Diese Frage behandelt - wie schon erwähnt - die Konsequenzen auf subjektiver Basis. 30% beantworteten die Frage mit der Gefahr der Demokratie. 23% nannten den Chilling-Effect, 20% waren der Meinung, das die Bürger immer Gläserner werden würden. 13% argumentierten, dass die Freiheit eingeschränkt werden würde und somit die Grundrechte nicht mehr geachtet werden würden. Ebenfalls 13% sahen keine negativen Konsequenzen auf den einzelnen. Die Freiheit des einzelnen kann jedoch ebenfalls als Gefahr für die Demokratie gesehen werden. Aufgrund dessen ist es nicht falsch, die Freiheit und die Gefahr für die Demokratie als eins anzusehen. Dieses Ergebnis lässt sich vermutlich ebenfalls in einer repräsentativen Studie feststellen. Rechnet man das Ergebnis von Frage 13 mit ein („Wieso wollen Sie sich schützen/nicht schützen), erlangt man das Ergebnis, das der Chilling-Effect mit der Gefährdung der Demokratie auf einer Stufe der Konsequenzen steht.
Genauer gesagt ist die Einschränkung der Meinungsfreiheit zum einen eine Gefahr für die Demokratie, aber auch ein weiterer Schritt in Richtung Chilling-Effect. Rechnet man also die 23% von der 13. Frage beim Chilling-Effect mit ein, könnte das Ergebnis bei einer groß angelegten Forschung anders aussehen als bei dieser explorativen Studie.



Die letzte Frage beschäftigt sich damit, ob und wie sehr die Überwachung ein Thema bei den Experten ist. Hier lag das Ergebnis bei 57% „ja, mich hat das Thema schon beschäftigt“ und 43% bei „nein, ich mache mir über die Überwachung keine Gedanken“.



12. Vergleich Experten, Passanten und der Verfasserin der Bachelor Arbeit

In diesem Kapitel soll der Vergleich zwischen den Passanten, den Experten und der Vermutung der Verfasserin stattfinden und die wichtigsten Unterschiede aufgezeigt werden.

Besondere Aufmerksamkeit bedürfen insoweit die Fragen 3 („Wie ist Ihre Meinung zur staatlichen Überwachung?), 6 (Was spricht für die staatliche Überwachung), 7 („Was spricht gegen die staatliche Überwachung?“), 12 („Wenn es um die Abwägung von Freiheit des einzelnen und die verstärkte Überwachung geht, welchen Schwerpunkt würden Sie dann setzen?“), 14 („wieso wollen Sie sich schützen/nicht schützen?“) und 18 („Welche Konsequenzen ergeben sich Ihrer Meinung schon heute daraus, dass der Staat den einzelnen in bestimmten Fällen überwacht?“), da hier die Unterschiede am deutlichsten zu erkennen sind.

Bei der Meinung zur staatlichen Überwachung waren 30% der Experten davon überzeugt, Überwachung wäre dann gut, wenn es einen Grund für diese gäbe. Bei den Passanten lag die größte Prozentzahl (26%) bei dem Argument „Nothing to Hide. Ebenfalls ist wichtig zu bemerken, dass keiner der Experten mit dem „zu geringen Wissen“ geantwortet hat. Logisch betrachtet ist dies nur die Konsequenz, wenn man Experte auf einem Gebiet ist. Insgesamt unterschieden sich die Meinungen zwischen Experten und Passanten bei dieser Frage deutlich. Während nur 16% bei den Passanten die Überwachung gut für die frühzeitige Erkennung von Verbrechen hielten, waren es bei den Experten 27%. Bei einer repräsentativen Studie könnte klar werden, dass die Experten das Thema Überwachung der Social-Media-Kommunikation eher nüchtern betrachten, während die Passanten sehr subjektiv und emotional bewerten. Hier wäre bei einer groß angelegten Studie im Einzelnen zu untersuchen, worauf die Unterschiede gründen, und insbesondere, ob schlicht das bessere Wissen auf Seiten der Experten die festgestellten Divergenzen erklären können.

Wenn dies so wäre, so bestünde eine Aufgabe der Medien und der Politik darin, die Allgemeinheit besser über den Sinn und Zweck und den Erfolg der Überwachung zu informieren und auf zu klären.

Eine weitere Frage die es genauer zu betrachten gilt, ist die sechste Frage. „Was spricht für die Überwachung der Social-Media-Kommunikation?“. Bei den Passanten waren 75% der Meinung, dass die Überwachung zur Prävention von Verbrechen geeignet ist. Die Experten waren zu 50% dafür. Die Zahl des „Nothing to Hide“ - Arguments war hier deutlich höher als bei den Passanten. Dies könnte die These bestätigen, dass die Experten das ganze Thema nüchterner betrachten. Nur 12% der Passanten brachten das „Nothing to Hide“ Argument an. Auf den ersten Blick erscheint nicht klar, inwieweit die unterschiedliche Einstellung von Passanten und Experten zur Eignung der Überwachung für die Prävention (vorherige Frage) im Einklang steht mit

dem Ergebnis zu dieser Frage, also im allgemeinen Argument für eine stärkere Überwachung. Hier müsste also im Rahmen einer repräsentativen und umfassenden Studie diese Eigenart des Ergebnisses der explorativen Studie durch intensivere Fragen näher beleuchtet werden.

Interessant bei dem Vergleich der siebten Frage („Was spricht gegen die staatliche Überwachung Social Media Kommunikation?“) ist folgendes: Die Experten nehmen hier die Privatsphäre augenscheinlich nicht all zu ernst, während die Passanten bei der Auswertung deutlich mehr von ihren Rechten spüren wollten. Lediglich 17% der Experten meinten, die Privatsphäre würde eingeschränkt. Deutlich größer (33%) viel die Antwort bei den Passanten aus. Bei der Freiheitseinschränkung war das Ergebnis umgekehrt. Hier antworteten 30% der Experten, das die staatliche Überwachung eine Freiheitseinschränkung mit sich bringen würde. Bei den Passanten jedoch waren nur 22% dieser Meinung. Dieses Ergebnis lässt sich auch bei den Konsequenzen wieder erkennen. 30% der Experten meinten, das nichts gegen Überwachung sprechen würde, während nur 20% der Passanten diese Meinung vertraten. Auch hier könnte eine repräsentative Studie im Einzelnen auf diesen Unterschied zielen.

Ein oft gehörter Satz von den Experten bei Frage 12 war folgender: Überwachung fängt da an, wo Sicherheit aufhört. Die Streitfrage ist hier jedoch, wann etwas aufhört und wo das andere beginnt. Hier gibt es viele Meinungen. Sobald ein Algorithmus das Wort „Bombe“ oder „Waffe“ aufgreift, könnte dies schon eine Gefährdung sein. Mehr dazu im Fazit. Bei oben genannter, zwölfter Frage, geht es um die Abwägung von Freiheit und Überwachung. 43% der Experten wollten sowohl Freiheit als auch Sicherheit. Dies funktioniert nur, wenn die Algorithmen Alarm schlagen, sobald bestimmte Keywords in den Konversationen auftauchen. Nur 20% der Passanten wollten den Mittelweg. 47%, und somit ein Großteil der Passanten, wollten die Freiheit des einzelnen mehr betonen als Sicherheit durch Überwachung. Nur 33% der Passanten waren der Meinung, das verstärkte Überwachung nötig sei. Wer von den beiden Parteien wirklich Recht hat, ist eine Frage der Einschätzung und vielleicht auch des Wissens.

Wie eine rote Linie zieht sich hier also die Skepsis der Passanten gegenüber einer stärkeren Überwachung durch die Antworten auf die verschiedenen Fragen; dies gilt allgemein, aber auch insbesondere beim Vergleich mit den Experten.

Wer viel weiß über die Überwachung der wird merken, dass Algorithmen bestimmte Keywords speichern und diese Konversationen an Mitarbeiter der NSA/CIA/BND etc. weiter leiten. Somit kann Überwachung - je nach Standpunkt - als zusätzliche Sicherheit und nicht als Einschränkung der Freiheit angesehen werden. Niemand weiß genau, wie viele Attentate durch diese Art der Überwachung verhindert werden konnten; immer wieder weißen staatliche Behörden darauf hin, dass Anschläge im Voraus erkannt und deshalb verhindert wurden. Hier wird unterstellt, dass solche Aussagen durch staatliche Behörden nicht erfunden werden.

„Wieso wollen Sie sich schützen/nicht schützen?“. Diese Frage ist eine der wichtigsten, wenn es um die Analyse der Konsequenzen geht. Hierbei stehen die Prozentzahlen von „Schützen: Meinungsfreiheit“ im Vordergrund. Dadurch kristallisiert sich heraus, ob der „Chilling-Effect“ als mögliche Konsequenz eintritt oder nicht. Dies könnte jedoch nur mit Sicherheit bei einer großen und repräsentativen Studie heraus gefunden werden.

Bei den Experten wollten sich 27% aufgrund der Meinungsfreiheit schützen, während es bei den Passanten nur 17% waren. 33% der Passanten wollten sich schützen, weil ihnen die Privatsphäre wichtig sei. 23% der Experten waren ebenfalls dieser Meinung. Somit könnte bei einer groß angelegten Forschung das Ergebnis sein, das die Passanten mehr im Chilling-Effect sind als die Experten. Denn diese meinten zu 33%, dass der Schutz nichts bringen würde, während die Experten nur zu 23% dieser Meinung waren. Hier ist zu vermuten, dass auf Seiten der Passanten eine diffuse Angst gemäß eines Gefühls der Unwissenheit zum Ausdruck kommt. Dies könnte in einer groß angelegten Studie näher überprüft werden.

Die letzte, zu betrachtende Frage, beschäftigt sich mit den direkten Konsequenzen. Im Gegensatz zu den Passanten war bei den Experten die Gefahr für die Demokratie mit 30% auf Platz eins, während bei den Passanten der Chilling-Effect mit 25% vorne lag. In einer repräsentativen Studie könnte dieses Ergebnis differenzierend hinterfragt werden. Zählt man noch das Ergebnis von Frage 14 dazu, erhöht sich das Ergebnis des Chilling-Effects bei beiden Gruppen erneut. 22% der Passanten waren der Meinung, dass die Bürger immer gläserner werden würden. Diese Meinung teilten nur 20% der Experten. Dieses Ergebnis lässt sich in einer repräsentativen Studie möglicherweise überprüfen. Im Sinne der der Notwendigkeit eines Grundvertrauens zwischen dem Bürger und dem Staat erscheint das Bewusstsein um den gläsernen Bürger schon derzeit also als problematisch; insoweit wäre zu klären, ob nicht der Staat die Aufgabe hat, mehr auf das Bewusstsein der Bürger Rücksicht zu nehmen, sei es durch stärkere Aufklärung oder auch durch eine partielle Rücknahme der Überwachung.

Vertieft sich in der Bevölkerung das Bild vom gläsernen Menschen, so hätte dies auf die Meinungsfreiheit und die Demokratie im Allgemeinen langfristig einen negativen Einfluss. Hier dürfte insbesondere die Vorratsdatenspeicherung in den Blick geraten.

Nun werden die Ergebnisse mit den Überlegungen von Sarah Schmidbauer verglichen. Wie im Literaturteil bereits erwähnt, sind die möglichen Konsequenzen der Überwachung der Chilling-Effect, die Gefährdung der Demokratie, die Einschränkung der Grundrechte im Allgemeinen und ein immer mehr werdender gläserner Bürger.

Diese Vermutungen konnten durch die explorative Studie bereits der Tendenz nach aufgezeigt werden. Wie das Ergebnis einer repräsentativen Studie sein könnte, wird erst am Ende klar werden. Hier zeigt sich also eine hinreichende Basis für den Inhalt und die Methode einer umfassenden Studie.

13. Beantwortung der Forschungsfrage

In diesem abschließenden Kapitel soll die Forschungsfrage beantwortet werden.

Insgesamt lässt sich sagen, dass die Meinung der Experten und die Meinung der Passanten nicht gleich sind. Dies lässt sich in einer repräsentativen Studie höchstwahrscheinlich bestätigen. Außerdem ist hier der Satz „Wissen ist Macht“ von großer Bedeutung. Die Passanten, die nicht allzu viel über das Thema wissen, argumentieren deutlich subjektiver und ihre Meinung wurde durch die Medien stark beeinflusst. Die Experten jedoch haben alle Fragen, die von Relevanz sind, neutraler betrachtet. Hierbei ist genau das Wissen der entscheidende Faktor. Denn Überwachung fängt da an, wo Sicherheit aufhört.

Ebenfalls ist zu bemerken, dass die Überwachung sowohl bei den Experten als auch bei den Passanten von erheblicher Bedeutung ist. In einer groß angelegten Forschung könnte dies ebenfalls deutlich zu sehen sein. Jeder befragte Passant im „Digital natives“ Alter konnte zu jeder Frage seine Meinung äußern. Diese waren - egal ob subjektiv oder nicht - meistens klar und deutlich.

Um die Forschungsfrage zu beantworten: Wie in der Literaturanalyse vermutet, könnten sowohl der Chilling-Effect als auch die Gefährdung der Demokratie mögliche Konsequenzen sein. Da diese Forschung von explorativer Art ist, kann dies nur endgültig in einer groß angelegten, repräsentativen Forschung herausgefunden werden. Jedoch könnten sich im weiteren Verlauf einige andere genannte Konsequenzen, wie zum Beispiel der gläserne Bürger oder die Freiheitseinschränkung, noch vor die Gefährdung der Demokratie stellen. Hier könnte eine große Studie den verlässlichen Nachweis erbringen.

Literaturverzeichnis - Internetquellen

15. Januar 2001 - Gründung Der Wikipedia
2011. http://www1.wdr.de/stichtag/stichtag5210.html, accessed September 28, 2017.

Andreas Von Gunten
2013a Überwachung Respektiert Die Würde Des Menschen Nicht. Andreas-vongunten.Com. https://andreasvongunten.com/blog/201378uberwachung-respektiert-die-wurde-des-menschen-nicht-html/, accessed October 5, 2017.

2013b Überwachung Respektiert Die Würde Des Menschen Nicht. Andreas-vongunten.Com. https://andreasvongunten.com/blog/201378uberwachung-respektiert-die-wurde-des-menschen-nicht-html/, accessed September 29, 2017.

Art 2 GG - Einzelnorm
N.d. https://www.gesetze-im-internet.de/gg/art_2.html, accessed September 9, 2017.

Bachelorarbeit Umfrage: Gestaltung, Aufbau, Auswertung
2017 Karrierebibel.De. https://karrierebibel.de/bachelorarbeit-umfrage/, accessed October 14, 2017.

Begriffsdefinition -Digitale Kommunikation, Online Kommunikation, Social Web
2014 Koorg. https://koorg.wordpress.com/2014/02/14/begriffsdefinition-digitale-kommunikation-online-kommunikation-social-web/, accessed October 9, 2017.

Bewegungs-Profile: Glasfaser-Kabel Werden Zur Überwachung Genutzt
DEUTSCHE WIRTSCHAFTS NACHRICHTEN. http://deutsche-wirtschafts-nachrichten.de/2014/01/07/bewegungs-profile-glasfaser-kabel-werden-zur-ueberwachung-genutzt/, accessed September 27, 2017.

Bildung, Bundeszentrale für politische Informationelle Selbstbestimmung | Bpb.
http://www.bpb.de/nachschlagen/lexika/recht-a-z/22392/informationelle-selbstbestimmung, accessed December 9, 2017.

Biselli, Anna
2013 NSA Für Dummies. Netzpolitik.Org. https://netzpolitik.org/2013/nsa-fuer-dummies-2/, accessed September 27, 2017.

Bundesamt Für Verfassungsschutz - Was Genau Macht Der Verfassungsschutz?
https://www.verfassungsschutz.de/de/das-bfv/aufgaben/was-genau-macht-der-verfassungsschutz, accessed November 9, 2017.

Bundesnachrichtendienst - Geschichte Des Bundesnachrichtendienstes Im Überblick

http://www.bnd.bund.de/DE/Organisation/Geschichte/Geschichte_Ueberblick/Timeline_node.html;jsessionid=69F43E42964C99C2C81359101F4C28CB.1_cid386, accessed December 9, 2017.

Bundesnachrichtendienst - HUMINT
http://www.bnd.bund.de/DE/Auftrag/Informationsgewinnung/HUMINT/humint_node.html, accessed October 28, 2017

BVerfG, Urteil Vom 15. Dezember 1983 - Az. 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (Volkszählungsurteil) https://openjur.de/u/268440.print, accessed October 6, 2017.

“Chilling Effect” - Massenüberwachung Zeigt Soziale Folgen
https://www.freitag.de/autoren/netzpiloten/massenueberwachung-zeigt-soziale-folgen, accessed October 6, 2017.

CIA - Bedeutung Erklärung Definition - Lexikon - CIA
http://www.info-magazin.com/?suchbegriff=CIA, accessed September 27, 2017.

Das Grundrecht Auf Informationelle Selbstbestimmung.Pdf
http://alt.staatundverwaltung.jura.uni-leipzig.de/sites/uni-leipzig.de.enders/files/Das%20Grundrecht%20auf%20informationelle%20Selbstbestimmung.pdf, accessed November 5, 2017.

Das Internet, ein überwachtes Zuhause
2013 sueddeutsche.de, http://www.sueddeutsche.de/digital/privatsphaere-das-internet-ein-ueberwachtes-zuhause-1.1746611-2, accessed October 19, 2017.

Datenschutz: Informationelle Selbstbestimmung in Theorie & Praxis | Das Datenschutz-Blog
https://www.datenschutzbeauftragter-online.de/datenschutz-antrittsvorlesung-michael-schmidl-informationelle-selbstbestimmung-theorie-praxis/5594/, accessed September 29, 2017.

Datenspuren Im Internet Und Den Sozialen Medien
2015 http://fczb.de/datenspuren-im-internet-und-den-sozialen-medien/, accessed September 27, 2017.

Datenspuren Und Datenschmutz
https://www.selbstdatenschutz.info/datenspuren, accessed September 27, 2017.

Der “Chilling Effect”: Massenüberwachung Zeigt Soziale Folgen - Netzpiloten.De, http://www.netzpiloten.de/der-chilling-effect-massenueberwachung-zeigt-soziale-folgen/, accessed September 27, 2017.

Die Entstehung von Whatsapp Geschichte
https://www.was-war-wann.de/geschichte/whatsapp.html, accessed September 27, 2017.

Die Unglaubliche Erfolgsgeschichte Des Whatsapp-Gründers
2014 Stern.De. http://www.stern.de/digital/telefon/jan-koum-die-unglaubliche-erfolgsgeschichte-des-whatsapp-gruenders-2091476.html, accessed October 19, 2017.

Echtzeit-Überwachung : So Funktioniert Das XKeyscore-Programm Der NSA - WELT
https://www.welt.de/politik/deutschland/article118593621/So-funktioniert-das-XKeyscore-Programm-der-NSA.html, accessed December 9, 2017.

Elisabeth & René Penselin
2015a Die Social Media Geschichte & Wie Es Weiter Geht, Kundengewinnung Im Internet. https://www.kundengewinnung-im-internet.com/social-media-geschichte/, accessed September 29, 2017.
2015b Die Social Media Geschichte & Wie Es Weiter Geht, Kundengewinnung Im Internet. https://www.kundengewinnung-im-internet.com/social-media-geschichte/, accessed September 29, 2017.

Facebook: Aktuelle Zahlen Zu Facebook (Q2/2017)
2017, http://www.thomashutter.com/index.php/2017/07/facebook-aktuelle-zahlen-zu-facebook-q22017/, accessed November 15, 2017.

Facebook-Geschichte Als Chronik - FOCUS Online
http://www.focus.de/digital/internet/facebook/tid-24930/die-geschichte-des-sozialen-netzwerks-facebooks-eroberung-der-welt-facebook-geschichte-als-chronik_aid_709860.html, accessed September 27, 2017.

Freiheit Oder Sicherheit?
Fluter.De. http://www.fluter.de/freiheit-oder-sicherheit, accessed October 12, 2017.

GmbH, Frankfurter Allgemeine Zeitung
2017 CIA Entblößt: Im Bett Mit Dem Spion. FAZ.NET. http://www.faz.net/1.4915084, accessed September 27, 2017.

Jan Koum: Die Unglaubliche Erfolgsgeschichte Des Whatsapp-Gründers | STERN.De
https://www.stern.de/digital/smartphones/jan-koum-die-unglaubliche-erfolgsgeschichte-des-whatsapp-gruenders-3411916.html, accessed December 9, 2017

Kuch, Alexander
So Wird Ein Glasfaser-Netz Überwacht. https://www.teltarif.de/glasfaser-netz-ueberwachung/news/68684.html?page=all, accessed September 27, 2017.

Lengsfeld, Autor Vera
Nothing to Hide? Big Brother Ist Bereits Unter Uns. Vera Lengsfeld. http://vera-lengsfeld.de/2017/01/10/nothing-to-hide-big-brother-ist-bereits-unter-uns/, accessed September 27, 2017.

Media-34000.Pdf
http://www.spiegel.de/media/media-34000.pdf, accessed October 6, 2017.

Menschenwürde | Grundrechteschutz
https://www.grundrechteschutz.de/gg/menschenwurde-2-255, accessed November 5, 2017.

Neues Gesetz Zur Online-Überwachung - Alle Fakten, Alle Wichtigen Fragen
http://www.rp-online.de/digitales/internet/neues-gesetz-zur-online-ueberwachung-alle-fakten-alle-wichtigen-fragen-aid-1.6898556, accessed September 27, 2017.

„Nothing to Hide": Der Totale Überwachungsstaat | Islamnixgut
N.d. https://nixgut.wordpress.com/2017/01/14/nothing-to-hide-der-totale-berwachungsstaat/, accessed September 27, 2017.

NSA: Was Ist Die National Security Agency Eigentlich? - Alle Infos Bei GIGA
http://www.giga.de/unternehmen/nsa-was-ist-die-national-security-agency-eigentlich/, accessed September 27, 2017.

NSA-Affäre: "Die Überwachung Verletzt Menschenrechte" | Amnesty International, https://www.amnesty.de/2013/10/28/nsa-affaere-die-ueberwachung-verletzt-menschenrechte, accessed September 29, 2017.

NSA-Programm XKeyscore: Diese Spähsoftware Findet Jedes Passwort | ZEIT ONLINE, http://www.zeit.de/digital/datenschutz/2015-08/bfv-verfassungsschutz-was-kann-xkeyscore/komplettansicht, accessed September 27, 2017.

Offizielle Nutzerzahlen: Instagram in Deutschland Und Weltweit
2017 Allfacebook.De. https://allfacebook.de/instagram/instagram-nutzer-deutschland, accessed December 9, 2017.

Online, FOCUS
USA – CIA, FBI, NSA, DEA. FOCUS Online, http://www.focus.de/politik/ausland/tid-32425/organisation-geschichte-spektakulaere-details-cia-mossad-bnd-so-spionieren-die-geheimdienste-der-welt_aid_1047674.html, accessed September 27, 2017.

Prantl, Heribert
2017 Bundestag will weitreichendes Überwachungsgesetz beschließen. sueddeutsche.de, June 22. http://www.sueddeutsche.de/digital/staatstrojaner-bundestag-will-weitreichendes-ueberwachungsgesetz-beschliessen-1.3554426, accessed September 27, 2017.

PRISM Und Tempora – SecuPedia
http://www.secupedia.info/wiki/PRISM_und_Tempora, accessed November 5, 2017.

Prism-Skandal: NSA Zahlte Facebook, Google Und Microsoft Millionenbeträge - Golem.De

https://www.golem.de/news/prism-skandal-nsa-zahlte-facebook-google-und-microsoft-millionenbetraege-1308-101177.html, accessed October 9, 2017.

Privatsphäre: Die Gefahren Des Sozialen Netzes - SPIEGEL ONLINE
http://www.spiegel.de/netzwelt/web/privatsphaere-die-gefahren-des-sozialen-netzes-a-517584.html, accessed September 27, 2017.

Recht Auf Informationelle Selbstbestimmung | Grundrechteschutz
https://www.grundrechteschutz.de/gg/recht-auf-informationelle-selbstbestimmung-272, accessed September 29, 2017.

Rixecker, Kim
5 Jahre WhatsApp: Zahlen Und Geschichte Des Messengers Im Überblick [Infografik]. T3n News. http://t3n.de/news/5-jahre-whatsapp-579623/, accessed September 27, 2017.

Sickert, Teresa
2016 Online-Überwachung: Was Das Neue BND-Gesetz Für Internetnutzer Bedeutet. Spiegel Online, October 19. http://www.spiegel.de/netzwelt/netzpolitik/bnd-gesetz-das-bedeutet-es-fuer-internetnutzer-a-1116940.html, accessed September 27, 2017.

Social Networking Und Privatsphäre
http://sicherheitskultur.at/privacy_soc_networking.htm, accessed September 27, 2017.

Solitonen
http://web.physik.uni-rostock.de/optik/de/for_kon_b_de.html, accessed September 27, 2017.

Staatliche Überwachung - Befallen Vom Überwachungsvirus
Deutschlandfunk. http://www.deutschlandfunk.de/staatliche-ueberwachung-befallen-vom-ueberwachungsvirus.1184.de.html?dram:article_id=307639, accessed October 12, 2017.

Staatliche Überwachung: Abhören, Orten, Ausspionieren Und Bespitzeln
https://www.selbstdatenschutz.info/staatliche_ueberwachung, accessed September 27, 2017.

Staatstrojaner: Wie Ermittler Eure WhatsApp-Nachrichten Verfolgen Könnten
http://www.huffingtonpost.de/2017/06/22/staatstrojaner-bundestag-uberwachungsgesetz_n_17257594.html, accessed September 27, 2017.

Stöcker, Christian
2013 Überwachungsprogramm Tempora: Es Geht Um Unsere Freiheit. Spiegel Online, June 23. http://www.spiegel.de/netzwelt/netzpolitik/kommentar-zu-tempora-ein-skandal-von-historischem-ausmass-a-907397.html, accessed September 27, 2017.

Überwachung Respektiert Die Würde Des Menschen Nicht | Andreasvongunten.Com
https://andreasvongunten.com/blog/201378uberwachung-respektiert-die-wurde-des-menschen-nicht-html/, accessed October 24, 2017.

US-Abhöraffäre: BND Nutzte Bislang Unbekanntes NSA-Spähprogramm | STERN.De
http://www.stern.de/politik/ausland/us-abhoeraffaere-bnd-nutzte-bislang-unbekanntes-nsa-spaehprogramm-3367132.html, accessed September 27, 2017.

Warum Es Moralisch Sein Kann, Die Eigenen Bürger Auszuspähen
N.d. http://www.tagesspiegel.de/meinung/usa-und-ueberwachung-warum-es-moralisch-sein-kann-die-eigenen-buerger-auszuspaehen/8334518.html, accessed November 15, 2017.

Was Ist Instant Messaging? Einfach Erklärt
http://praxistipps.chip.de/was-ist-instant-messaging-einfach-erklaert_41407, accessed October 29, 2017

Was Ist Instant Messaging? Einfach Erklärt - CHIP
http://praxistipps.chip.de/was-ist-instant-messaging-einfach-erklaert_41407, accessed Novomber 9, 2017.

Was Ist Online-Kommunikation?
2013 Magronet - Online Marketing Blog. http://www.magronet.de/online-kommunikation/, accessed September 27, 2017.

Weinberger, Matt
Diese Fotos Zeigen, Wie Facebook von Einem Wohnheim-Projekt Zum Tech-Giganten Wurde. Business Insider Deutschland. http://www.businessinsider.de/die-geschichte-von-facebook-in-bildern-2016-9, accessed September 27, 2017.

Welche Formen von Kommunikation Kann Man Unterscheiden? Vor- Und Nachteile? | Karteikarten Online Lernen | CoboCards
https://www.cobocards.com/pool/de/card/8xv9f0314/online-karteikarten-welche-formen-von-kommunikation-kann-man-unterscheiden-vor-und-nachteile-/, accessed September 27, 2017.

Literaturverzeichnis - Bücher

Kielholz, Annette
2008, Titel: Online-Kommunikation - Die Psychologie der neuen Medien für die Berufspraxis: E-Mail, Website, Newsletter, Marketing, Kundenkommunikation. Springer Science & Business Media, 4. Auflage, Springer Verlag

Orwell, George
Juni 1994, Titel: 1984, 3. Auflage, Ullstein Verlag

Rosenbach, Marcel; Stark, Holger
2014, Titel: Der NSA-Komplex: Edward Snowden und der Weg in die totale Überwachung

Greenwald, Glenn
2014, Titel: Die globale Überwachung - Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen, 1. Auflage, Droemer-Knauer-Verlag

Anlagen

Interviewleitfaden Sarah Schmidbauer

Ziel und Funktion:

- Meinung über die Nutzung der Social-Media-Kommunikationaufgrund der staatlichen Überwachung.
- Erfassung, wie Experten und Passanten mit ihren Daten im Facebook Messenger und WhatsApp umgehen
- Meinung zum Thema Selbstbestimmungsrecht
- Zukunftsprognose über zukünftiges Verhalten

Methode:
Umfrage von 60 Passanten und 30 Experten. Explorative Studie

Zielgruppe:
Bei Experten: Menschen die über ein überdurchschnittliches Wissen zum Thema „staatliche Überwachung“ verfügen - unter anderem Polizisten, Redakteure und Politiker
Bei Passanten: „Digital Natives“

Sachthemen:
I. persönliche Einstellung und Wissen zum Thema staatliche Überwachung der Social-Media-Kommunikation
II. persönliche Einstellung zum Thema Datenschutz in den Sozialen Netzwerken
III. Meinung zum Thema Selbstbestimmungsrecht
IV. Mögliche Folgen der Überwachung -> siehe Hypothese

Fragen
I. Persönliche Einstellung und Wissen zum Thema staatliche Überwachung und Social-Media-Kommunikation

- Nutzen Sie Facebook-Messenger? Warum?
- A:
- Nutzen Sie WhatsApp? Warum?
- A:
- Wie ist Ihre Meinung zur staatlichen Überwachung der Social-Media-Kommunikation?
- A:
- Nutzen Sie Facebook/WhatsApp prozentual gesehen mehr für geschäftliche oder private Zwecke? Warum?
- A:
- Was spricht für, was gegen die staatliche Überwachung der Social-Media Kanäle
- A:
- Stört Sie Überwachung? Wenn ja warum, wenn nein warum nicht?
- A:

- Stört Sie auch ein allgemeines Gefühl der Überwachung, selbst wenn sie dazu nichts im einzelnen Wissen?
- A:
- Würde es Sie auch stören, wenn möglicherweise das Telefon überwacht, wenn ja, warum?
- A:
- Gehen Sie davon aus, das unsere Rechtsordnung im ganzen Staat zu viele Möglichkeiten der Informationssammlung über den einzelnen einräumt?
- A:
- Glauben Sie, das staatliche Überwachung bei der Prävention von Vergehen und Verbrechen hilft?
- A:
- Wenn es um die Abwägung von verstärkter Überwachung und der Freiheit des einzelnen geht, welchen Schwerpunkt würden Sie dann setzen?
- A:

II. Persönliche Einstellung zum Thema Datenschutz auf Facebook Messenger und WhatsApp

- Wie schützen Sie sich in den Messengern vor der staatlichen Überwachung?
- A:
- Wieso wollen Sie sich schützen/nicht schützen?
- A:
- Geben Sie persönliche Daten auf Facebook und WhatsApp von sich preis?
- A:

III. Meinung zum Thema Selbstbestimmungsrecht

- glauben sie das es wichtig ist für Sie, das ausschließlich Sie selbst, darüber bestimmen, welche Daten der Staat über Sie sammelt und wie der Staat diese Daten verwendet
- A:
- Glauben Sie, dass dieses Recht in der Wirklichkeit umsetzbar ist?
- A:

IV. Welche Folgen hat Überwachung

- Welche Konsequenzen ergeben sich nach ihrer Meinung schon heute daraus, das der Staat in bestimmten Fällen den einzelnen Überwacht?
- A:

Anlage 2: E-Mail an Experten

Sehr geehrte Damen und Herren, mein Name ist Sarah Schmidbauer. Im Moment schreibe ich meine Bachelorarbeit zu folgendem Thema: Beeinflusst die staatliche Überwachung der Social-Media-Kommunikationdas Verhalten junger Nutzer.
Hierfür habe ich einen Fragebogen erstellt, den sie bitte ausgefüllt an mich zurück senden, um die Antworten mit denen der Passanten zu vergleichen.
Herzliche Grüße
Sarah Schmidbauer

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe. Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Ort, Datum	Vorname Nachname