

Die Gefahren von Big Data für die Demokratie und die rechtlichen Herausforderungen

BACHELORARBEIT

zur Erlangung des akademischen Grades

Bachelor of Science

im Rahmen des Studiums

Wirtschaftsinformatik

eingereicht von

Betül Sezer

Matrikelnummer 01633057

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Wien, 21.02.2021

Betül Sezer

Markus Haslinger

Erklärung zur Verfassung der Arbeit

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Aus Gründen der leichteren Lesbarkeit wird in der vorliegenden Bachelorarbeit die gewohnte männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung des weiblichen Geschlechts, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

Wien, 21.02.2021

Sezer Betül

Abstract

Big Data and Big Data Analytics become more and more important as the amount of data is permanently increasing. For organizations data has become the most important resource. Companies use Big Data to understand their customers better and to make better business decision based on the result of big data analytics. This technology can be used in many ways. Data of any kind can be both beneficial and damaging. With all the data we are producing on the internet, it is possible for organizations and the governments to monitor or manipulate people. There are a lot of cases of data breaches and scandals every year, which cause misuse of personal data of millions of people. Political campaigns use voter databases with specified information about individual citizens for profiling. It is very important for all organizations and for governments to have a data strategy and a data protection policy. Tech giants like Facebook and Twitter, which gather a lot of data, must be monitored independently for data protection. Any company and organization that stores or processes data of EU citizen must comply with the General Data Protection Regulation (GDPR), which protects personal data of individuals in the EU. As the misuse of personal data increases with the amount of data, data protection becomes more important. This paper discusses the risks of Big Data and gives an overview of the GDPR and the Data Protection Law of Austria.

Inhaltsverzeichnis

1. Einleitung	1
2. Big Data	4
2.1. Was ist Big Data?	5
2.2. Big Data Mining	7
2.2.1. Mustertypen	7
2.3. Big Data Analytics	8
2.3.1. Predictive Analytics	9
2.3.2. Descriptive Analytics	9
2.3.3. Diagnostic Analytics	10
2.3.4. Prescriptive Analytics	10
2.4. Big Data Technologien	10
2.4.1. Apache Hadoop	10
2.4.2. NoSQL-Datenbanken	12
2.4.3. In-Memory-Datenbanken	14
3. Big Brother – die Überwachungsstaaten	15
3.1. Digitaler Autoritarismus in China	15
3.1.1. The Great Firewall von China	16
3.1.1.1. Das Prinzip der GFW	16
3.1.2. Internet in China heute	19
3.1.3. Big Data wird zu Big Brother	21
3.1.4. Das Sozialkreditsystem (SKS)	21
3.1.4.1. Datensammlung des SKS	22
3.1.4.2. Das Bestrafungsmechanismus	24
3.2. Überwachung in Russland	26
3.2.1. SORM – System für operative Ermittlungsaktionen	26
3.2.2. Russland und China im Vergleich	27
3.3. Überwachung in Europa	28
3.3.1. Deutschlands BND-Spionageaffäre	28
3.3.2. Das TEMPORA-Programm des britischen Geheimdiensts	29
4. Politische Kampagnen und Big Data	30
4.1. Cambridge Analytica und Facebook-Datenskandal	30
4.2. Datenaggregation	31
4.2.1. Datenermittlung über Facebook und die Friends API	32
4.3. Politisches Microtargeting	34
4.3.1. OCEAN-Scoring	34
4.4. Rechtliche Konsequenzen	36

5. Gefahren von Big Data	38
5.1. Manipulation	38
5.2. Massenüberwachung	39
5.3. Die große Macht der Technologieunternehmen	40
5.4. Probleme der Big Data Analytics	41
6. Rechtliche Herausforderungen	43
6.1. Europäische Datenschutzgrundverordnung (DGSVO)	43
6.1.1. Grundsätze für die Verarbeitung personenbezogener Daten	44
6.1.2. Rechtmäßigkeit der Verarbeitung	45
6.1.3. Bedingungen für die Einwilligung	46
6.1.4. Verarbeitung besonderer Kategorien personenbezogener Daten	47
6.1.5. Informationspflicht	48
6.1.6. Profiling	49
6.1.7. Technische Maßnahmen zur sicheren Datenverarbeitung	50
6.1.8. Datenschutz-Folgenabschätzung	51
6.2. Datenschutzgesetz in Österreich	52
6.2.1. Grundrecht auf Datenschutz	52
6.2.2. Datengeheimnis	53
6.2.3. Datenverarbeitungen zu spezifischen Zwecken	53
6.2.4. Bildverarbeitung	54
6.2.5. Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei	56
7. Conclusio	57
8. Anhang	I
9. Literaturverzeichnis	II
10. Abbildungsverzeichnis	X

Abkürzungsverzeichnis

BND	Bundesnachrichtendienst
CAP	Consistency, Availability und Partition
DSG	Datenschutzgesetz
DSGVO	Datenschutzgrundverordnung
DNS	Domain Name System
FTC	Federal Trade Commision
FSB	Föderalen Sicherheitsdienst
GSR	Global Science Research
GCHQ	Government Communications Headquarters
GPS	Global Positioning System
HDFS	Hadoop Distributed File System
HTTP	Hypertext Transfer Protocol
IDC	International Data Corporation
ICO	Information Commissioner's Office
IoT	Internet of Things
ISP	Internet Service Provider
KI	Künstliche Intelligenz
KPC	Kommunistischen Partei Chinas
NCISP	National Credit Information Sharing Platform
NSA	National Security Agency
OCEAN-Scoring	Openness - O, Conscientiousness – C, Extroversion - E, Agreeableness – A und Neuroticism – N
RAM	Random Access Memory
RDBMS	Relationales Datenbank-Managementsystem
RIPA	Regulation of Investigatory Powers Act
SCL Group	Strategic Communication Laboratories Group
SKS	Sozialkreditsystem
SORM	Systems für Ermittlungsaktivitäten
GFW	The Great Firewall
URL	Uniform Resource Locator
VPN	Virtual Private Network
YARN	Yet Another Resource Negotiator

1. Einleitung

In dieser zunehmend digitalisierten Welt hinterlassen wir eine Datenspur mit allem was wir machen, sei es eine Suche nach einem bestimmten Wort, Kauf eines Kleidungsstückes online, oder das Staubsaugen mit einem Saugroboter. Im April 2020 betrug die Zahl der Internetnutzer 4,57 Milliarden Menschen, welche 59 Prozent der Weltbevölkerung ausmacht.¹ Die Daten kommen nicht nur aus dem Verhalten der Personen im Internet, sondern auch aus all den Sensoren der Smart-Geräten, wie Smartphones, Saugroboter, etc. Das Internet der Dinge (Internet of Things – IoT) prägt unseren Alltag. Diese Technologie ermöglicht die Verbindung der physischen Objekte mit dem Internet. Eine Prognose von Cisco besagt, dass im Jahr 2023 über 14,7 Milliarden Geräte vernetzt sein werden, was bedeutet, dass **es** immer mehr Daten generiert werden.² Es ist jedoch auch wichtig, einen Mehrwert aus diesen Daten zu schaffen und dies geschieht mit Big Data Analytics.

Unternehmen verwenden Big Data, um das Verhalten ihrer Kunden besser zu verstehen und somit besser ihren Wünschen nachzukommen. Mithilfe von Big Data Analytics versuchen Unternehmen die Kundenzufriedenheit zu erhöhen, indem sie ihre Kunden anhand der erfassten Daten über deren Verhalten mit personalisierten ansprechen. Es gibt Algorithmen, die die Personen auf den Bildern erkennen, gesprochene Worte verstehen, sie in geschriebene Texte übersetzen und deren Inhalt auf Bedeutung und Stimmung analysieren, wie zum Beispiel können Algorithmen aus einzelnen Wörtern erkennen, ob die Kundenbewertungen negativ oder positiv sind. An diesem Punkt kommt die Künstliche Intelligenz (KI) ins Spiel, doch um ein gutes Ergebnis zu erzielen, sind gute und qualitative Daten eine Voraussetzung. Mithilfe von Big Data Technologien ist es möglich, die Daten so zu verarbeiten, um einen Nutzen daraus zu erzielen.

Big Data hat das Potenzial, die Art und Weise, wie Unternehmen und Organisationen ihre Entscheidungen treffen, wesentlich zu verändern. Big Data Analysen bieten eine verbesserte Entscheidungsgrundlage für das Management. Beispielsweise können Fragen wie „Welche Auswirkung hat eine Preiserhöhung in einem bestimmten Markt?“ oder „Welcher Markt wäre offen für eine Innovation?“ mittels Big Data Analytics innerhalb kurzer Zeit beantwortet werden. Die kurze Auswertungszeit und die hohe Qualität der Auswertungen ermöglichen ein wesentliches Sparen an Kosten und Zeit. Patientenbezogene Gesundheits- und medizinische Daten können dafür verwendet werden, um ein besseres Verständnis der medizinischen Befunde zu erlangen.³ Die Analysetechniken können dem Arzt während des

¹ Vgl. Domo (20.12.2020). Data never sleeps 8.0

² Vgl. Cisco (2020), S. 8

³ Vgl. Raghupathi & Raghupathi (2014), S. 2

Entscheidungsprozesses dabei helfen, die beste geeignete Behandlungsweise für den jeweiligen Patienten festzustellen und anzuwenden.

Nach der Automatisierung der Produktion und der Schaffung selbstfahrender Autos erleben wir die größte Transformation seit dem Ende des zweiten Weltkriegs.⁴ Wir hören viel von datengetriebenen Geschäftsmodellen, Entscheidungen, Produkten, etc. Heute gilt China als Beispiel für eine datengesteuerte Gesellschaft. Jeder chinesische Bürger soll einen Sozialkredit erhalten, der darüber entscheidet, ob diese Person für einen Kredit, Job, oder ein Visum qualifiziert ist oder nicht. Das will die Volksrepublik China mit den, durch die Massenüberwachung der Bevölkerung erfassten Daten, ermöglichen. George Orwells Roman „1984“ wird also Realität. Auch andere Länder wie Russland haben ein System integriert, mit dem es ihre Bevölkerung überwacht bzw. abhört. Die Überwachung in diesen Ländern ist aufgrund der Gesetzeslage möglich, was nach der Datenschutzgrundverordnung in Europa nicht zulässig ist.

Politische Kampagnen basieren heutzutage ebenfalls auf Big Data Auswertungen. Der Cambridge Analytica und Facebook-Datenskandal zeigt uns, welche Möglichkeiten Big Data bietet und damit die Demokratie gefährdet. Der Datenmissbrauch, die Datenweitergabe und mangelnder Datenschutz in den Sozialen Medien stellt ebenfalls eine große Gefahr für die Gesellschaft dar.⁵

Hiermit kommen wir zum Datenschutz, das eines der wichtigsten Themen bei der Arbeit mit den Daten. Die Datenschutzgrundverordnung (DSGVO) regelt europaweit den Datenschutz und in Österreich wird diese um das Datenschutzgesetz (DSG) ergänzt. Nicht nur für Organisationen, die Daten verarbeiten, sondern auch für individuelle Person ist es besonders wichtig, sich mit dem Datenschutz zu beschäftigen und sich über die Rechte und Pflichten zu informieren.

Diese Bachelorarbeit befasst sich mit Big Data und die Risiken von Big Data für die Demokratie und Gesellschaft. Mit den Themen wie Massenüberwachung, Microtargeting und Profiling in der Politik werden die Problemfelder der Big Data Analytics aufgegriffen und die rechtliche Grundlage des Datenschutzes in Europa und Österreich näher erläutert.

Das erste Kapitel definiert Begriffe wie Big Data, Data Mining und Big Data Analytics und hat auch das Ziel, die Leser über die bekanntesten und wichtigsten Big Data Technologien aufzuklären.

Im weiteren Teil der Arbeit werden die Überwachungstechniken der Länder China, Russland, Deutschland und Großbritannien erläutert. Die Geschichte des Internets in China und dessen Entwicklung im 21. Jahrhundert wird untersucht und das Prinzip der Great Firewall von China beschrieben. Das Sozialkreditsystem und das

⁴ Vgl. Helbing (2019), S. 74ff

⁵ Vgl. Fuchs (2010), S. 457

Internet heute in China werden auf technischer und rechtlicher Grundlage näher analysiert. Es werden zusätzlich auf die Überwachungstechniken von Russland eingegangen und ein Vergleich zwischen den beiden Ländern, Russland und China, aufgestellt. Auch die Enthüllungen von Edward Snowden werden im Weiteren erwähnt und die Überwachung in Europa auf Grundlage der Enthüllungen wird erklärt.

Das nächste Kapitel beschäftigt sich damit, wie Cambridge Analytica im Wahlkampf in den US-Präsidentenwahlen 2016 die Facebook-Daten von Millionen amerikanischen Bürgern missbraucht hat. Die dabei verwendeten Techniken werden ebenfalls näher erläutert. Im Anschluss werden die rechtlichen Konsequenzen für Facebook und Cambridge Analytica nach der Enthüllung des Skandals dargelegt.

Basierend auf das zweite und dritte Kapitel werden im nächsten Teil der Arbeit die Risiken von Big Data und Big Data Analytics zusammengefasst und analysiert. Dabei wird darauf eingegangen, wie Big Data und Big Data Analytics eine Massenüberwachung durch den Staat ermöglichen und welche Rolle dabei die Social-Media-Unternehmen spielen. Es werden weiteres auch die große Macht dieser Social-Media-Unternehmen in Frage gestellt.

Eine wichtige Rolle spielt der Umgang mit dieser großen Menge an Daten und hier kommt der Datenschutz in Frage. Die Erfassung, Speicherung, Weitergabe und Verarbeitung der Daten in Europa regelt die DSGVO und in Österreich noch zusätzlich das DSG. In welchen Umständen die Erfassung, Speicherung, Weitergabe und Verarbeitung der Daten möglich ist und unter welchen Voraussetzungen der Staat ihre Bürger überwachen kann, wird in diesem Kapitel erläutert.

Zum Abschluss werden Verbesserungspotenziale für den Umgang mit Big Data und die Nutzung der Big Data Analytics analysiert.

2. Big Data

„Personenbezogene Daten sind das neue Öl des Internets und die neue Währung der digitalen Welt.“⁶

Dieses bekannte Zitat der EU-Politikerin Meglena Kuneva von 2009 war schon in aller Munde, bevor das Wort *Big Data* die digitale Welt dominierte. In dieser zunehmenden digitalen Welt, die einen enormen Fortschritt im Jahr 2020 durch den Ausbruch von COVID-19 erreicht hat, spielen Daten viel mehr Rolle im Alltag eines Menschen. In Bezug auf den Bericht „Data never sleeps 8.0“ von DOMO, ein cloud-basiertes Softwareunternehmen, wurden in 2020 jede Minute auf den Plattformen wie

- Zoom 208.333 Teilnehmer in Meetings aufgezeichnet,
- Netflix 404.444 Stunden Videos übertragen,
- Youtube 500 Stunden Videos hochgeladen,
- Instagram 138.889 Werbungen in Business-Profilen angeklickt,
- Facebook 147.000 Bilder hochgeladen,
- etc.⁷

Die International Data Corporation (IDC) erwartet 2025, dass die global erzeugte Datenmenge auf 163 ZB⁸ wachsen wird, welche dieses Jahr mit dem hohen Anstieg der Digitalisierung durch die COVID-19-Pandemie 59 ZB beträgt.^{9 10} Diese Daten werden immer von entscheidender Bedeutung des menschlichen Lebens, denn sie ändern unseren Alltag, sie beeinflussen unsere Entscheidungen und die Art und Weise, wie wir die Welt erleben.

Im folgenden Kapitel wird der Begriff Big Data und die Technologien dahinter näher erläutert.

⁶ Vgl. Kuneva (2009)

⁷ Vgl. Domo (20.12.2020). Data never sleeps 8.0

⁸ Zettabytes sind eine Milliarde Terabytes. 1 ZB = 1.000.000.000.000.000.000 Bytes

⁹ Vgl. Reinsel et al., (2017), S. 5

¹⁰ Vgl. IDC (20.12.2020). IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data

2.1. Was ist Big Data?

Um den Begriff Big Data zu verstehen, sollten zuerst die Arten von Daten erklärt werden. Daten werden in strukturierte, unstrukturierte und semi-strukturierte Daten unterteilt.

Strukturierte Daten sind Daten, die in Datenbanken gespeichert und in Zeilen und Spalten gegliedert werden können, wobei jede Zeile ein Datensatz und jede Spalte ein Feld indiziert.¹¹ Diese Daten können beispielsweise durch eine Registrierung generiert werden (Name, E-Mail-Adresse, Passwort). Die unstrukturierten Daten hingegen machen die Daten aus, die nicht einfach zu kategorisieren sind, wie Fotos, Videos, Tweets, Chatverläufe und Textdokumente.¹² Diese unstrukturierten Daten können nicht identifiziert werden, wobei zum Beispiel durch ein Hashtag ein Tweet kategorisiert und durch einen Betreff oder Sender auf eine E-Mail verwiesen werden kann.¹³ Diese Daten werden semi-strukturierte Daten genannt. Daten, wie Hashtags oder Betreff einer E-Mail, die auf bestimmte Daten verweisen, werden Metadaten genannt. Die Metadaten werden verwendet, um den unstrukturierten Daten eine gewisse Struktur zu geben.¹⁴

Big Data umfasst zusätzlich die Daten, die unstrukturiert in Form von Text, Fotos und Bildern sind, nicht mit den traditionellen Methoden der strukturierten Datenanalyse analysiert werden können und daher neue algorithmische Techniken benötigen, um nützliche Informationen zu erheben.¹⁵

Gartner, ein IT-Beratungs- und Marktforschungsunternehmen, definiert Big Data als einen großen (Volume), schnellen (Velocity) und/oder vielfältigen (Variety) Informationsbestand.¹⁶ Doug Laney, ein Branchenanalyst, entwickelte in 2001 das 3-V-Modell, welches die Begriffe Volume, Velocity und Variety in Bezug auf Big Data beschreibt.

Volume

Das Volumen beschreibt den Umfang des Datenbestandes, der im Bereich Tera- bis Zettabyte liegt. Zur Übersicht, um wie viele Bytes es sich bei Tera- bis Zettabyte handelt:¹⁷

- Gigabyte = 10^9 Byte
- Terabyte = 10^{12} Byte

¹¹ Vgl. Holmes (2017), S. 4

¹² Vgl. Holmes (2017), S. 5

¹³ Vgl. Holmes (2017), S. 5

¹⁴ Vgl. Holmes (2017), S. 5

¹⁵ Vgl. Holmes (2017), S. 5

¹⁶ Vgl. Gartner (22.12.2020). Glossar – Big Data

¹⁷ Vgl. Fasel & Meier (2016), S. 6

- Petabyte = 10^{15} Byte
- Exabyte = 10^{18} Byte
- Zettabyte = 10^{21} Byte

Velocity

Big Data umfasst all die Arten von Daten, die strukturiert, unstrukturiert und semi-strukturiert sind.¹⁸ Mittels Big Data Algorithmen können auch komplexe Daten ausgewertet und analysiert werden.

Variety

Die Geschwindigkeit in diesem Zusammenhang beschreibt die Echtzeitverarbeitung von ausgewerteten und analysierten Daten.¹⁹

Später wurden zwei weitere Begriffe eingeführt und das 3-V-Modell wurde zu einem 5-V-Modell weiterentwickelt.

Value

Mit Big Data Anwendungen soll der Wert eines Unternehmens gesteigert werden. Hier können beispielsweise mit Big Data Technologien analysiert werden, in welchen Bereichen eines Unternehmens investiert werden muss, um einen Mehrwert zu schaffen.²⁰

Veracity

Dieser Begriff beschreibt in diesem Zusammenhang die Aufrichtigkeit und Wahrhaftigkeit der Daten.²¹ Aufgrund des Umfangs dieser Daten und der unterschiedlichen Quellen, kann die Qualität der Daten nicht garantiert werden. Daher ist es bei der Datenverarbeitung wichtig, dass es mit den richtigen Daten gearbeitet wird, um inkonsistente Ergebnisse zu vermeiden.

Das 5-V-Modell stellt grundlegende Herausforderungen dar und bringt auch viele Vorteile mit sich. Diese Herausforderungen und Vorteile können durch Data Mining verständlich gemacht werden.

¹⁸ Vgl. Fasel & Meier (2016), S. 6

¹⁹ Vgl. Fasel & Meier (2016), S. 6

²⁰ Vgl. Fasel & Meier (2016), S. 6

²¹ Vgl. Fasel & Meier (2016), S. 6

2.2. Big Data Mining

Um den Wert der Daten zu verstehen, müssen diese zuerst verarbeitet werden und um einen hohen Wert zu erreichen, müssen die nützlichen und wertvollen Informationen aus massiven Datensätzen gefiltert werden. Mithilfe von Data Mining und Machine-Learning-Methoden ist es möglich, die richtigen und wertvollen Informationen aus Big Data zu extrahieren. Data Mining ermöglicht durch mathematisch-statistische Verfahren zur Datenanalyse, die Erkennung bisher unbekannter Zusammenhänge, Muster und Trends aus großen Datensätzen und eine Vorhersage auf Basis von generierten Modellen.²² Begriffe wie Muster und Merkmale sind im Rahmen von Data Mining sehr wichtig. Der Begriff Muster umfasst entscheidende Ausprägungen von Merkmalen in den Daten.²³ Weiteres ist der Begriff Merkmale in diesem Zusammenhang als Inputgrößen von Problemstellungen zu verstehen.²⁴

2.2.1. Mustertypen

Für die Erkennung von Mustern in Daten gibt es vier verschiedene Mustertypen, die für Data Mining entsprechend sind.

Klassifizierungs- und Vorhersageregeln

Dieser Mustertyp zielt darauf, Beschreibungen der Klassen zu erstellen, mit den Informationen, die dieser Klassen zugeteilt wurden.²⁵ Durch Vorhersageregeln soll das zukünftige Verhalten von Objekten generiert werden.²⁶ Ein Beispiel dafür ist die Risikobewertung der Lebensversicherung. Hier sind die Eigenschaften wie Raucher bzw. Nicht-Raucher oder das Alter ein Klassifikationsfaktor. In diesem Beispiel beschreibt die Prognose der Versicherungsprämien eine Schätzung von Werten.

Abweichungsregeln

Hier wird versucht durch Vergleich der früheren und aktuellen Werten Anomalien in bestimmten Kennzahlen zu entdecken. Um eine Erklärung dieser Abweichungen zu finden, wird die Datenbasis auf kausale Zusammenhänge geprüft.²⁷ Auf Basis dieser Informationen können Abweichungsregeln gebildet werden, welche die Abweichungen zwischen bestimmten Variablen beschreiben.

²² Vgl. Farkisch (2011), S. 97

²³ Vgl. Farkisch (2011), S. 97

²⁴ Vgl. Farkisch (2011), S. 97

²⁵ Vgl. Farkisch (2011), S. 98

²⁶ Vgl. Farkisch (2011), S. 98

²⁷ Vgl. Farkisch (2011), S. 98

Aufdeckung von Beziehungsmustern

Zwischen den Objekten, die mehrmals in Transaktionen vorkommen, existiert eine Beziehung. Ein Beziehungsmuster entsteht beim häufigen Auftritt dieser Beziehungen.²⁸ Solche Beziehungsanalysen werden beispielsweise in der Telekommunikation eingesetzt, wo für jeden Anruf eine logische Verknüpfung zwischen Teilnehmern geschaffen wird.²⁹ Es werden auch insbesondere Abhängigkeitsanalysen durchgeführt, womit die Häufigkeit des Vorkommens der Objekte, die in einer Transaktion auftreten, ermittelt wird. Um das Verhalten der Objekte in einem Zeitverlauf zu beobachten und bestimmte sequenzielle Muster zu analysieren, werden Zeitreihenanalysen angewendet.³⁰

Segmente (Cluster)

Die Clusteranalyse gruppiert ähnliche Objekte, wodurch Cluster entstehen. Ein Beispiel für die Anwendung dieser Analyse ist die Erstellung von Zielgruppen zur gezielter Wahlwerbung beim Wahlkampf.³¹

Zusammengefasst ist die wesentliche Aufgabe des Data Minings die Datenverarbeitung und -auswertung, um Muster und Modelle in den Daten zu entdecken und zu generieren, die später bei der Herleitung von Daten, die bei der Entscheidungsbildung eine relevante Rolle spielen, eingesetzt werden können.

2.3. Big Data Analytics

Big Data Analytics befassen sich mit der Extraktion von verwertbarem Wissen und Erkenntnissen aus Big Data. Sie spiegeln die Herausforderungen von umfangreichen, unstrukturierten und schnellen Daten wider, um sie mit traditionellen Methoden zu verwalten. Die Gewinnung von nützlichen Informationen aus riesigen Datenmengen ist für Organisationen weltweit immer wichtiger geworden. Der Versuch, schnell und einfach aussagekräftige Erkenntnisse aus solchen Datenquellen zu gewinnen, ist eine Herausforderung. Daher ist es fast unmöglich geworden, ohne Big Data Analytics den vollen Wert von Big Data auszuschöpfen. Die Tools, die für den Umgang mit dem Volumen, der Geschwindigkeit und der Vielfalt von Big Data zur Verfügung stehen, haben sich in den letzten Jahren stark verbessert. Die vier Arten von Datenanalyse und die wichtigsten Big Data Technologien werden im folgenden Kapitel erläutert.

²⁸ Vgl. Farkisch (2011), S. 99

²⁹ Vgl. Farkisch (2011), S. 99

³⁰ Vgl. Farkisch (2011), S. 99

³¹ Vgl. Farkisch (2011), S. 100

2.3.1. Predictive Analytics

Die prädiktive Analyse verwendet Technologien, die maschinelles Lernen, statistische Modellierung und Data Mining umfassen.³² Predictive Analytics wird verwendet, um die Steigerung des Umsatzes, Prüfungsergebnisse, Finanzdienstleistungen, soziale Netzwerke, Betrugserkennung, Telekommunikation, Mobilität und andere Bereiche zu analysieren.³³ Hier wird versucht, die Frage „*Was wird wahrscheinlich passieren?*“ zu beantworten.³⁴ Mit dieser Methode werden die Informationen aus den verfügbaren Datensätzen extrahiert. Diese gefilterten Informationen werden dann verwendet, um die Möglichkeit zu prognostizieren, die in der Zukunft mit der Risikoanalyse und -minderung passieren kann.³⁵ Da es sich hier nur um eine Prognose handelt, werden korrekte Ergebnisse der allen vorhergesagten Daten nicht garantiert. Die bekannteste Anwendung, die in der prädiktiven Analyse verwendet wird, ist das Kreditscoring.³⁶ Diese Form von Analytik wird sowohl in den sozialen Medien als auch im digitalen Marketing, beispielsweise in der Werbung, angewendet. Wenn der User mit bestimmten Produkten und Werbungen interagiert und dieser später ähnliche Werbungen von dem bestimmten Produkt überall im Feed zu sehen bekommt, steckt eine Form von prädiktiver Analytik im Hintergrund.³⁷

2.3.2. Descriptive Analytics

Die deskriptive Analyse wird verwendet, um die Fragen „*Was ist passiert?*“ und „*Was passiert gerade?*“ zu beantworten.³⁸ Mit deskriptive Analytics werden vergangene Ereignisse aufgegliedert, wobei diese Ereignisse sich auf jeden beliebigen Zeitpunkt beziehen können.³⁹ Diese historischen Daten werden danach zusammengefasst, um Muster zu identifizieren. Diese Form von Analyse ist sehr wertvoll, da sie den Organisationen ermöglicht, aus vergangenen Methoden zu profitieren und die Auswirkung auf zukünftige Ergebnisse zu erkennen. Beispiele für die deskriptive Analyse sind Aufzeichnungen von Organisationen, die einen Rückblick auf ihre Finanzen, Kunden und Verkäufe geben, oder auch die Summe von Likes, Kommentaren und Posts in sozialen Medien.⁴⁰ Auch die Social-Media-Analytics sind hauptsächlich deskriptiv.⁴¹ Am Ende geht es darum, die bestmöglichen Entscheidungen zu treffen.

³² Vgl. Raj, et al., (2020), S. 8

³³ Vgl. Raj, et al., (2020), S. 8

³⁴ Vgl. Gartner (25.12.2020). Glossar – Predictive Analytics

³⁵ Vgl. Raj, et al., (2020), S. 8

³⁶ Vgl. Raj, et al., (2020), S. 8

³⁷ Vgl. Gonçalves (2017), S. 292

³⁸ Vgl. Gartner (25.12.2020). Glossar – Descriptive Analytics

³⁹ Vgl. Raj, et al., (2020), S. 9

⁴⁰ Vgl. Raj, et al., (2020), S. 10

⁴¹ Vgl. Gonçalves (2017), S. 291

2.3.3. Diagnostic Analytics

Die diagnostische Analyse beschäftigt sich mit der Frage „*Warum ist das passiert?*“ und zielt damit darauf, die Grundursache von Problemen zu finden.⁴² Techniken wie Data Discovery, Korrelationen und Data Mining können angewendet werden, um die Frage „*Warum?*“ zu beantworten. Es ist eine Methode zum Verstehen des Auftretens von Ereignissen und Verhaltensweisen.⁴³ Als Beispiel kann hier die Zurückverfolgung von der Grundursache des Rückgangs eines Website-Traffics eines Unternehmens angegeben werden, welcher als Folge einen Rückgang der Verkäufe aufweist.⁴⁴

2.3.4. Prescriptive Analytics

Bei der präskriptiven Analyse geht es um die Frage „*Was wäre, wenn ...?*“, das heißt, sie beschäftigt sich damit, wie sich bestimmte Verhaltensweisen auf ein Ergebnis auswirken.⁴⁵ Hier wird ebenfalls Künstliche Intelligenz (KI) angewendet, um diese Fragen zu beantworten. Die präskriptive Analytics verwenden deskriptive und prädiktive Analyse, da sowohl mathematische Verfahren verwendet werden, um das gewünschte Ergebnis zu filtern, als auch Analysetechniken eingesetzt werden, um Vorhersagen zu treffen.⁴⁶ Unternehmen wollen mit der prädiktiven Analyse wirtschaftliche Beziehungen besser verstehen und prognostizieren können, um die Auswirkungen einzelner Entscheidungen zu entdecken und zu bewerten.

2.4. Big Data Technologien

Aufgrund der zahlreichen Herausforderungen im Bereich großer Datenmengen (Volume), einer großen Datenvielfalt (Variety), einer hohen Geschwindigkeit der Datengenerierung (Velocity), der Aufrichtigkeit der Daten (Veracity) und der Erreichung des Mehrwerts der Daten (Value) gibt es verschiedene Big Data Lösungen, die diese Herausforderungen in verschiedenen Bereichen ansprechen.

2.4.1. Apache Hadoop

Apache Hadoop ist eine Open Source Implementation und gehört zu den wichtigsten Big Data Technologien. Mithilfe von Hadoop können große Datenmengen leicht verarbeitet und auf vielen Rechnern in einem System gespeichert werden. Ein Vorteil davon ist, dass keine teure Hardware benötigt werden, da auch normale

⁴² Vgl. Gartner (25.12.2020). Glossar – Diagnostic Analytics

⁴³ Vgl. Raj, et al., (2020), S. 11

⁴⁴ Vgl. Raj, et al., (2020), S. 11

⁴⁵ Vgl. Raj, et al., (2020), S. 12

⁴⁶ Vgl. Raj, et al., (2020), S. 12

Computer verwendet werden können, deren Server mit Verwendung von Hadoop um weitere Knoten erweitert werden.⁴⁷ Hier spricht man von Scale-Out-Effekt.⁴⁸

Eine weitere Komponente von Apache Hadoop ist das Hadoop Distributed File System. HDFS ermöglicht die Speicherung großer Datenmengen, bei denen es sich um semi-strukturierte und unstrukturierte Daten handelt.⁴⁹ Bei der Verwendung von HDFS sind die Daten auf viele Rechner im Cluster verteilt, die sich physisch in Rechenzentren auf der ganzen Welt befinden.⁵⁰ Ein HDFS-Cluster besteht aus zwei Nodes, einem Master-NameNode und einem Slave-DataNode, die verschiedene Aufgaben übernehmen. Der NameNode behandelt alle eingehenden Anfragen, verteilt den Speicherplatz und behält den Überblick über die Verfügbarkeit und den Speicherort der Daten.⁵¹ Weiteres übernimmt er auch die einfachen Operationen, wie das Öffnen und Schließen von Dateien, und kontrolliert den Datenzugriff.⁵² Die DataNodes verwalten das Speichern von Daten und erstellen, löschen und replizieren dadurch Blöcke nach Bedarf.⁵³ Das Replizieren von Daten ist eine wichtige Eigenschaft von HDFS. Ein Vorteil von HDFS gegenüber einer relationalen Datenbank ist die Speicherung riesiger Datenmengen. Facebook beispielsweise verwendet HDFS, um seine stets wachsende Datenmenge zu speichern.⁵⁴

Ein weiteres Programmiermodell von Apache Hadoop ist das Hadoop Map Reduce. Dieses Modell kann große Berechnungen aufgrund der Verteilung der Daten auf mehrere Rechner in angemessener Zeit ausführen, was die Map-Funktion des Modells übernimmt. Die Reduce-Funktion führt danach die Teilergebnisse zusammen.⁵⁵ Ein Vorteil dieses Verfahrens ist die hohe Ausfallsicherheit.⁵⁶ Im Vergleich zu relationalen Datenbankmanagementsystemen (RDBMS) benötigt Map Reduce jedoch etwas länger bei Durchführung von Abfragen.⁵⁷

Die Komponente YARN (Yet Another Resource Negotiator) verwaltet alle Ressourcen, die in einem Cluster gespeichert sind. Nach dem Start einer Anwendung, werden die benötigten Ressourcen, wie CPU, RAM und Festplatten, der Anwendung zugeteilt, um den Start der Prozesse dieser Anwendung zu ermöglichen.⁵⁸

⁴⁷ Vgl. Schön (2016), S. 310

⁴⁸ Vgl. Schön (2016), S. 310

⁴⁹ Vgl. Holmes (2017), S. 31

⁵⁰ Vgl. Schön (2016), S. 309

⁵¹ Vgl. Holmes (2017), S. 31

⁵² Vgl. Holmes (2017), S. 31

⁵³ Vgl. Holmes (2017), S. 31

⁵⁴ Vgl. Holmes (2017), S. 32

⁵⁵ Vgl. Schön (2016), S. 310

⁵⁶ Vgl. Schön (2016), S. 310

⁵⁷ Vgl. Schön (2016), S. 310

⁵⁸ Vgl. Fasel & Meier (2016), S. 130

2.4.2. NoSQL-Datenbanken

NoSQL ist der Oberbegriff für nicht-relationale Datenbanken und steht für Not only SQL.⁵⁹ NoSQL-Datenbanken zeichnen sich dadurch aus, dass sie unstrukturierte Daten, wie Bilder und Videos, besser verwalten und verarbeiten können. Sie sind nicht relational und speichern eine große Menge von Daten.⁶⁰ Eine weitere wichtige Eigenschaft der nicht-relationalen Datenbank ist die horizontale Skalierbarkeit, also das Hinzufügen weiterer Server, was eine bessere Leistung und eine einfachere Replikation der Daten ermöglicht.⁶¹ Bei umfangreichen Anwendungen mit unstrukturierten Daten ist jedoch der Fall, dass nicht die Konsistenz, sondern die kurze Reaktionszeit, die Ausfalltoleranz und die Verfügbarkeit der Daten im Vordergrund stehen.⁶² Der Grund für dieses Problem kann mit dem CAP-Theorem erklärt werden.⁶³

CAP-Theorem

Laut dem CAP-Theorem können nicht die drei Eigenschaften Konsistenz (Consistency), Verfügbarkeit (Availability) und Ausfalltoleranz (Partition Tolerance) gleichzeitig erfüllt werden.⁶⁴

- Konsistenz (Consistency)

Nach einer Operation auf Daten muss die Konsistenz der Daten erhalten bleiben, das heißt, alle Knoten, die eine Lese- bzw. Schreibzugriff auf diesen Knoten haben, müssen aktualisiert werden. Dies bedeutet jedoch eine längere Reaktionszeit aufgrund der Vielzahl an Knoten, die über die Aktualisierung informiert werden müssen.⁶⁵

- Verfügbarkeit (Availability)

Hierbei soll jeder nicht ausgefallene Knoten eine Antwort für alle Lese- und Schreib Anforderungen innerhalb einer angemessenen Zeit liefern können. Verfügbarkeit eines Knotens bedeutet, dass alle Knoten akzeptable Antwortzeiten haben.⁶⁶

- Ausfalltoleranz (Partition Tolerance)

Eine gute Ausfalltoleranz benötigt Replikationen von Daten, denn ohne Replikationen, kann ein Ausfall eines Knotens das System beeinträchtigen. Ausfalltoleranz

⁵⁹ Vgl. Holmes (2017), S. 32

⁶⁰ Vgl. Schön (2016), S. 308

⁶¹ Vgl. Schön (2016), S. 308

⁶² Vgl. Schön (2016), S. 308

⁶³ Vgl. Fasel & Meier (2016), S. 31

⁶⁴ Vgl. Schön (2016), S. 308

⁶⁵ Vgl. Schön (2016), S. 308

⁶⁶ Vgl. Schön (2016), S. 308

bedeutet, dass ein System auch mit einem ausgefallenen Knoten problemlos weiterarbeiten kann.⁶⁷

Da eine Datenbank nicht alle drei Eigenschaften erfüllen kann, gibt es drei Systemarten für Datenbanken. Die Abbildung 1 stellt die Zusammenhänge dieser Eigenschaften dar.

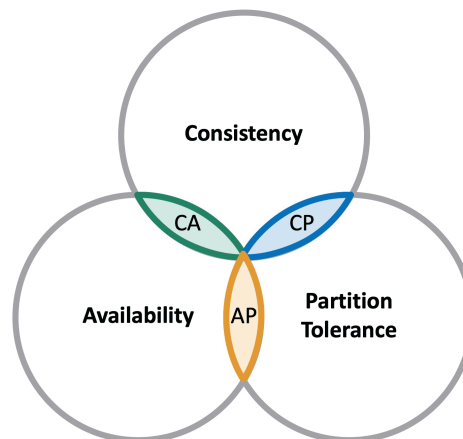


Abbildung 1: CAP-Theorem⁶⁸

- CP-System

Ein CP-System bevorzugt die Konsistenz und die Ausfalltoleranz und verzichtet auf die Verfügbarkeit.⁶⁹ Im Finanzwesen ist dieses System sehr wertvoll, da in den Bankanwendungen die Konsistenz und die Ausfallsicherheit von Überweisungen sehr wichtig sind, um Fehlbuchungen auszuschließen.

- AP-System

Diese Systemart verzichtet hingegen auf die Konsistenz und unterstützt die Eigenschaften Verfügbarkeit und Ausfalltoleranz. Hier wird die Aktualisierung der Daten verzögert.⁷⁰ Es kann bis zu mehreren Stunden bzw. Tagen dauern, bis alle Knoten aktualisiert werden.

- CA-System

Hierbei werden die zwei Eigenschaften Konsistenz und Verfügbarkeit unterstützt. Diese Systemart ist in den relationalen Datenbanken zu finden, da sie mehr nach Konsistenz und Verfügbarkeit streben.⁷¹

⁶⁷ Vgl. Schön (2016), S. 308

⁶⁸ Vgl. HazelCast (27.12.2020). Glossar – CAP-Theorem

⁶⁹ Vgl. Schön (2016), S. 309

⁷⁰ Vgl. Schön (2016), S. 309

⁷¹ Vgl. Schön (2016), S. 309

2.4.3. In-Memory-Datenbanken

Bei In-Memory-Datenbanken, anstatt Daten wie bei relationalen Datenbank-Managementsystemen (RDBMS) auf Festplatten zu speichern, werden sie auf dem Hauptspeicher hinterlegt.⁷² Diese Technik ermöglicht sowohl einen schnelleren Abruf von Daten als auch eine Beschleunigung der Datenanalysen. Neben vielen Vorteilen bringt diese Technik auch Nachteile mit sich. Im Fall eines Systemausfalls können alle nicht geschützten Daten am Hauptspeicher verloren gehen.⁷³ Um diese Gefahr zu vermeiden, bietet es sich ein Hybrid-In-Memory-System an. Diese Form von Datenbank speichert nur ein Teil der Daten auf dem Hauptspeicher und den Rest, wie bei üblichen Datenbanken, auf der Festplatte.⁷⁴ Hierbei werden die relevanten Daten, auf die mehrmals zugegriffen wird, im Hauptspeicher gespeichert, um eine schnellere Auswertung bzw. Verarbeitung dieser Daten zu ermöglichen.⁷⁵

⁷² Vgl. Schön (2016), S. 307

⁷³ Vgl. Schön (2016), S. 307

⁷⁴ Vgl. Schön (2016), S. 307

⁷⁵ Vgl. Schön (2016), S. 307

3. Big Brother – die Überwachungsstaaten

Big Data wird auch unter anderem zur Überwachung der Gesellschaft verwendet. China entwickelt ein Sozialkreditsystem, mit dem es darauf zielt, die soziale Vertrauenswürdigkeit seiner Bevölkerung und der Unternehmen zu ermitteln. Mittels Big Data und immense Überwachung sollen das Verhalten der Bürger, Unternehmen und Institutionen erfasst und bewertet werden.⁷⁶

In der COVID-19-Pandemie wurden in vielen Ländern neue Überwachungstechnologien eingesetzt, die davor als zu aufdringlich angesehen wurden. Die Krise hat die Digitalisierung, Sammlung und Analyse der persönlichen Daten der Bevölkerung ohne angemessenen Schutz vor Missbrauch mit sich gebracht. Regierungen und private Einrichtungen setzten verstärkt Big Data Technologien und biometrische Überwachung ein, um Entscheidungen zu treffen, die die wirtschaftlichen, sozialen und politischen Rechte der Menschen beeinflussen.⁷⁷

In den folgenden Abschnitten werden digital-autoritäre Staaten und deren Systeme zur Überwachung der Bevölkerung erläutert.

3.1. Digitaler Autoritarismus in China

Lacie Pound, eine junge Dame, deren durchschnittliche Bewertung 4,3 ist, verbringt ihre Zeit damit, bezaubernde Fotos für ihr Social-Media-Profil zu machen und andere Menschen per einer Mensch-Mensch-Rating-App zu bewerten.

Als sie ihr Traumhaus findet, wird sie von ihrem Makler über ein Programm informiert, das ihr 20 Prozent Rabatt auf die Miete gibt, wenn sie eine Bewertung über 4,5 hat. Dann bittet sie eine alte Freundin die Trauzeugin bei ihrer Hochzeit zu sein, und aufgrund der Tatsache, dass sie dort mit einer guten Rede ihr Rating verbessern kann, nimmt sie die Anfrage ihrer Freundin an. Von seinem Bruder, mit dem sie einen Streit hatte und einem Taxifahrer, den sie warten gelassen hatte, wird sie jeweils mit einem Stern bewertet. Nach den schlechten Bewertungen fällt ihr Rating unter 4,2, was es ihr unmöglich macht, einen Flug zum Hochzeitsort zu finden, da ihre Anfragen durch die Fluggesellschaften aufgrund ihrer niedrigen Bewertung abgelehnt werden.

Diese Geschichte spielt sich in einer Folge der britischen Science-Fiction-Serie Black Mirror ab, die in 2011 von Charlie Brooker ins Leben gerufen wurde.⁷⁸ Diese

⁷⁶ Vgl. WKO (06.11.2020). China führt ab 2021 ein Social Credit System für Unternehmen ein

⁷⁷ Vgl. Freedom House (06.11.2020). The Pandemic's Digital Shadow

⁷⁸ Vgl. Black Mirror, "Nosedive", Staffel 3, Folge 1 (2016)

Serie untersucht die moderne Gesellschaft im Hinblick auf den Einfluss und die Auswirkungen der Verwendung der neuen Technologien.

Diese Fantasie wird jedoch wahr. China ist auf dem Weg ein Sozialkreditsystem für die ganze Bevölkerung einzuführen.

3.1.1. The Great Firewall von China

In 1994 kam das Internet unter dem Staatspräsidenten Jiang Zemin nach China, da er damals nach Alvin Tofflers Theorie der dritten Welle, die besagt, dass sich die Welt vom Industriezeitalter (zweite Welle) zum Informationszeitalter (dritte Welle) bewegt, davon überzeugt war, dass China nur dann im Wettbewerb mit anderen Ländern bestehen kann, wenn das Internet im Land zugänglich ist.⁷⁹

*"Wenn man das Fenster für frische Luft öffnet, muss man damit rechnen, dass ein paar Fliegen hineinfliegen."*⁸⁰ Nach diesem Grundsatz vom ehemaligen Staatspräsidenten Deng Xiaoping wurde das Projekt „Der Goldene Schild“ - auch „The Great Firewall“⁸¹ (GFW) genannt - in 1996 gestartet, um das Land von diesen „Fliegen“ abzugrenzen. Dieses Projekt zerstörte die Ideologie von Zemin, der durch das Einführen des Internets im Land mit dem Westen im Wettbewerb stehen wollte.⁸² Die Absicht der chinesischen Regierung hinter diesem GFW-Projekt besteht lediglich darin, falsche Informationen, die von außerhalb des Landes stammen, zu filtern und zu blockieren, um die Gesellschaft vor ihrem Einfluss zu schützen.⁸³ Seit seiner Einführung vor zwei Jahrzehnten hat sich das Projekt weiterentwickelt und zu einem hochsicheren, stark überwachten System geworden. Mittlerweile sind tausende Webseiten blockiert, unter anderem auch Seiten wie Google, Facebook, Twitter, Youtube, WhatsApp, etc.⁸⁴

Um die Firewall zu überwinden, wenden sich die Menschen in China der Nutzung von VPN-Anwendungen zu, jedoch gibt es hier auch ein hartes Vorgehen der Regierung, wie zum Beispiel hohe Geldstrafen oder auch Haftstrafen, gegen VPN-Anbieter und -Benutzer.⁸⁵

3.1.1.1. Das Prinzip der GFW

Alle Internetdiensteanbieter in China werden vom Ministerium für Industrie und Informationstechnologie lizenziert und kontrolliert, was bedeutet, dass jeder Inhalt in und aus China von den chinesischen Behörden überwacht und manipuliert werden

⁷⁹ Vgl. Torfox, A Stanford Project (10.11.2020). The Great Firewall of China: Background

⁸⁰ Deng Xiaoping (1904-1997)

⁸¹ Vgl. Wired (12.11.2020). The Great Firewall of China

⁸² Vgl. Torfox, A Stanford Project (10.11.2020). The Great Firewall of China: Background

⁸³ Vgl. Chandel, et al., (2019), S.114

⁸⁴ Vgl. BBC (11.11.2020). Social Media and Censorship in China: how is it different to the West?

⁸⁵ Vgl. The Guardian (13.11.2020). Man in China sentenced to five years jail for running VPN

kann. Unter der GFW wurden mehrere Methoden eingesetzt, um eine Auffangmaßnahme zu ermöglichen.⁸⁶

DNS-Poisoning

Eine der primären Filtermethoden, die die GFW verwendet, ist das Poisoning von DNS-Antworten für bestimmte Domänen. Wenn eine DNS-Anfrage durch die GFW empfangen wird, sendet sie eine vergiftete DNS-Antwort an den anfragenden DNS-Resolver, das heißt, dass die Firewall falsche IP-Adressen zurückgibt und dadurch die Webseiten unzugänglich macht.⁸⁷

URL-Filtering

Die GFW besteht auch aus einem URL-Filtersystem, das den Zugriff auf die Webseite blockiert, obwohl die URL nicht auf der schwarzen Liste der Regierung – Liste der verbotenen Webseiten – steht.⁸⁸ Das Filtersystem untersucht den HTTP-Verkehr daraufhin, ob bestimmte Schlüsselwörter vorhanden sind, die die chinesische Regierung verboten hat. Diese Schlüsselwörter beziehen sich wie zum Beispiel auf politische Ideologien, die die Regierung für inakzeptabel hält, oder auf historische Ereignisse, die das Regime nicht diskutiert haben möchte.⁸⁹

Selbstzensur

Chinesische Unternehmen sind dazu verpflichtet, ihre Inhalte nach den Gesetzen und Vorschriften der Regierung zu gestalten. Verstöße gegen jegliche Gesetze führen zu harten Strafen, wie hohe Bußgelder oder Betriebsstilllegungen.⁹⁰ Das Gesetz für Internet- und Informationsdiensteanbieter ist unter Artikel 15 der „Maßnahmen für die Verwaltung von Internet und Informationsdiensteanbieter“⁹¹ geregelt und dieses besagt, dass *„Anbieter von Internet-Informationsdiensten keine Informationen produzieren, bei der Produktion helfen, herausgeben oder senden dürfen,*

- I. die sich den Grundprinzipien, wie sie in der Verfassung bestätigt sind, widersetzen;*
- II. die die Sicherheit der Nation gefährden, Staatsgeheimnisse preisgeben, die Staatsgewalt untergraben oder die Integrität der Einheit der Nation gefährden;*
- III. die der Ehre oder den Interessen der Nation schadet;*

⁸⁶ Vgl. Medium (12.11.2020). How it works: The Great Firewall of China

⁸⁷ Vgl. Farnan, et al., (2016), S. 95

⁸⁸ Vgl. Chandel, et al., (2019), S. 114

⁸⁹ Vgl. OpenNet (12.11.2020). OpenNet Initiative: Bulletin 005 – Probing Chinese Search Engine Filtering

⁹⁰ Vgl. Chandel, et al., (2019), S. 114

⁹¹ Vgl. Art 15 Maßnahmen für die Verwaltung von Internet- und Informationsdiensteanbieter 2000, Staatsrat der Volksrepublik von China

- IV. *die zu ethnischer Feindseligkeit und ethnischer Diskriminierung aufstacheln oder die Einheit zwischen ethnischen Gruppen gefährden;*
- V. *die der Religionspolitik des Staates schaden oder Sekten oder feudalen Aberglauben befürworten;*
- VI. *die Gerüchte verbreiten, die soziale Ordnung stören oder die soziale Stabilität schädigen;*
- VII. *die Obszönität, Pornographie, Glücksspiel, Gewalt, Mord und Terror verbreiten oder zu Verbrechen aufstacheln;*
- VIII. *die andere beleidigen oder verleumden oder deren gesetzliche Rechte und Interessen verletzen;*
- IX. *oder andere Inhalte enthalten, die durch Gesetz oder Verwaltungsvorschriften verboten sind.*⁹²

Manuelle Durchsetzung

Viele Zivilangestellte sind in China damit beschäftigt, um verbotene Inhalte im Internet zu filtern. Diese Angestellte überwachen Online-Inhalte, und die, die von der Regierung als schädlich für den Fortschritt Chinas angesehen werden, werden an die Behörden gemeldet.⁹³ Die jüngsten Fortschritte in der KI-Technologie hat es mittlerweile ermöglicht, die Überwachungsprozesse größtenteils zu automatisieren.⁹⁴

Blockieren von VPN

Um die Firewall zu überwinden, ist das Virtual Private Network (VPN) ein Muss für die Internetnutzer in China. Mit diesem System werden VPN-ähnliche Datenverkehr erkannt und diese Verbindungen unterbrochen, sodass die Internetnutzer sich nicht mit ausländischen Servern verbinden können. In 2017 startete das Ministerium für Industrie und Informationstechnologie eine umfassende Initiative zur Abschaltung nicht autorisierter Internetverbindungen, wie das VPN.⁹⁵ Eine eingeschränkte interne Nutzung von VPNs durch Unternehmen ist mit einem Nutzungshinweis zulässig. Die erforderlichen Systeme werden nur von speziell lizenzierten Anbietern geliefert.⁹⁶

⁹² Vgl. Art 15 Maßnahmen für die Verwaltung von Internet- und Informationsdiensteanbieter 2000, Staatsrat der Volksrepublik von China

⁹³ Vgl. Chandel, et al., (2019), S. 114

⁹⁴ Vgl. Chandel, et al., (2019), S. 114

⁹⁵ Vgl. Reuters (13.11.2020). China cracks down on unauthorized internet connections

⁹⁶ Vgl. Xiao (2019) S. 56

3.1.2. Internet in China heute

Die GFW von China ist mittlerweile so weit entwickelt, dass das Internet in China auch „Chinanet“ genannt wird.⁹⁷ Im März 2020 erreichte China 904 Millionen Internetnutzer.⁹⁸ Das ist die größte Population von Internetnutzern auf der ganzen Welt und das macht China zum Land mit dem größten digitalen Markt der Welt.⁹⁹ Zum Vergleich gibt es in den USA 298 Millionen Internetnutzer.¹⁰⁰ In der Abbildung 2 ist der Vergleich zwischen der chinesischen und der US-amerikanischen Internetnutzung zu sehen. Während die Internet-Abdeckungsrate von China bei 63 Prozent liegt, beträgt sie in den USA 90 Prozent.¹⁰¹ Die chinesische Population von Internetnutzern ist in einem Jahr um 75 Millionen Nutzer gestiegen, wobei in den USA ein Zuwachs von 5 Millionen zu sehen ist.¹⁰² Als Grund für diesen hohen Zuwachs von Internetnutzern in China wird die COVID-19-Pandemie gesehen.¹⁰³

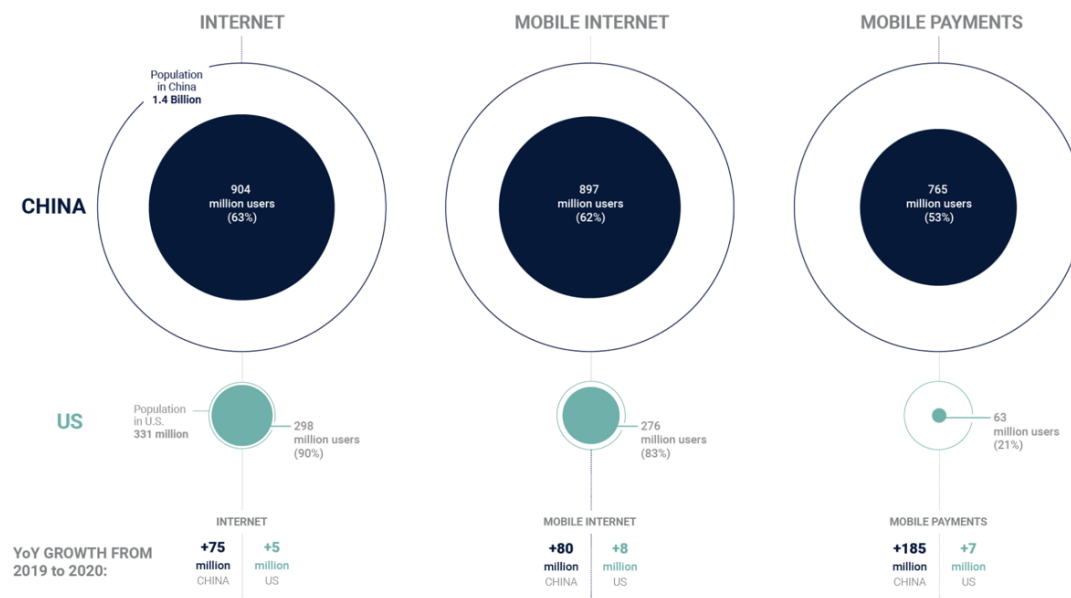


Abbildung 2: China vs U.S. Internet¹⁰⁴

Die Auswirkungen des Ausbruchs von COVID-19 haben Chinas Pläne zur digitalen Infrastruktur beschleunigt, wobei sowohl die Zentralregierung als auch der Technologiesektor einen bedeutenden Beitrag leistet.¹⁰⁵

⁹⁷ Vgl. TED Talk (16.11.2020). Behind the Great Firewall of China

⁹⁸ Vgl. Statista (16.11.2020). Number of internet users in China from December 2008 to March 2020

⁹⁹ Vgl. Wirtschaftswoche. (16.11.2020). Warum China zum Entwicklungsland wird

¹⁰⁰ Vgl. SCMPR (2020), S. 4

¹⁰¹ Vgl. SCMPR (2020), S. 4

¹⁰² Vgl. SCMPR (2020), S. 4

¹⁰³ Vgl. SCMPR (2020), S. 12

¹⁰⁴ Vgl. SCMPR (2020), S. 4

¹⁰⁵ Vgl. SCMPR (2020), S. 15

Im Februar 2020 führte China eine nationale Initiative ein, eine App, um das Coronavirus einzudämmen.¹⁰⁶ Die App weist der chinesischen Bevölkerung farbige QR-Codes zu, um festzustellen, ob sie unter Quarantäne gestellt werden müssen. Das farbbasierte System basiert auf Faktoren wie Reiseverlauf, Dauer des Aufenthalts in einem von dem Ausbruch betroffenen Gebiet und Beziehungen zu potenziellen Virusträgern.¹⁰⁷ Die App funktioniert nach der Eingabe einer nationalen Identitätsnummer und einer Telefonnummer. Danach werden Nutzer aufgefordert einen Fragebogen über Reiseverlauf und aktuelle Symptome auszufüllen. Nach Auswertung des Fragebogens werden dann den Nutzern eine Farbe zugewiesen. Dieser Gesundheitscode kann die Farbe Grün haben, welches bedeutet, dass die Person gesund ist. Gelb bedeutet, dass die Person mit einer anderen Person, die aktuell erkrankt ist, in Kontakt war. Rot sagt aus, dass die Person in die Quarantäne gehen muss.¹⁰⁸ Die Gesundheitscodes können auch als Tracker für die Bewegungen von Menschen in öffentlichen Bereichen dienen, da die Anwohner ihre QR-Codes beim Betreten öffentlicher Orte scannen lassen müssen. Sobald ein bestätigter Fall diagnostiziert wird, können die Behörden schnell zurückverfolgen, wo sich der Patient aufgehalten hat, und Personen identifizieren, die mit dieser Person in Kontakt standen.¹⁰⁹ Nach welchen Kriterien und wie diese App die Personen klassifiziert, wurde jedoch von der chinesischen Regierung nicht im Detail erklärt.¹¹⁰

Nach mehreren Analysen des Systems konnte jedoch erkannt werden, dass die Daten, die mittels dieser Contact-Tracing-App erhoben werden, auch mit der Polizei ausgetauscht werden und damit eine Vorlage für neue Formen der automatisierten sozialen Kontrolle geschaffen wird, die lange nach der Pandemie bestehen bleiben können.¹¹¹ Ob die erhobenen persönlichen Daten in einem zentralen Server gespeichert werden, ist nicht bekannt.¹¹² Falls diese Daten, die mittels dieser App erhoben werden, in einer zentralen Datenbank gespeichert werden, heißt das, dass die Regierung Zugriff auf diese Daten hat. Das Teilen von persönlichen Daten mit den Behörden benötigt keine Verständniserklärung der Appnutzer.¹¹³

Die chinesische Stadt Hangzhou plant eine solche App, die zum Contact-Tracing in der COVID-19-Pandemie eingeführt wurde, zu einem festen System zur Verfolgung

¹⁰⁶ Vgl. CNN (17.11.2020). China is fighting the coronavirus with a digital QR-Code. Here is how it works

¹⁰⁷ Vgl. SCMPR (2020), S. 16

¹⁰⁸ Vgl. CNN (17.11.2020). China is fighting the coronavirus with a digital QR-Code. Here is how it works

¹⁰⁹ Vgl. CNN (17.11.2020). China is fighting the coronavirus with a digital QR-Code. Here is how it works

¹¹⁰ Vgl. The New York Times (17.11.2020). In Coronavirus Fight, China gives Citizens a Color Code, With Red Flags

¹¹¹ Vgl. The New York Times (17.11.2020). In Coronavirus Fight, China gives Citizens a Color Code, With Red Flags

¹¹² Vgl. Norton Rose Fulbright (2020), S. 2

¹¹³ Vgl. Norton Rose Fulbright (2020), S. 2

der Gesundheit der Bevölkerung zu machen.¹¹⁴ Die Daten sollen mit zusätzlichen Gesundheitsindikatoren erweitert werden, um eine individuelle Index-Rankings von der Gesundheit der Person zu entwickeln. Solche Indikatoren könnten unter anderem Schlafstunden, Schrittzahl, gerauchte Zigaretten oder das Trinken von Alkohol sein. Während das Konsumieren von Alkohol die Punktzahl verringert, erhöht eine Schrittzahl von 10.000 Schritten die Punktzahl.¹¹⁵

3.1.3. Big Data wird zu Big Brother

Die Regierung von China hat mehrere Datenplattformen aufgebaut, die bevölkerungsweite Daten sammeln, speichern und nutzen. Eine dieser Plattformen ist die National Credit Information Sharing Platform (NCISP), die mit mehreren Regierungsbehörden und Marktakteuren verbunden ist.¹¹⁶ Es ist bekannt, dass auch High-Tech-Firmen wie Alibaba und Baidu, Daten mit der NCISP austauschen.¹¹⁷ Die Big Data Technologien werden von der Regierung eingesetzt, um das wirtschaftliche, politische und soziale Verhalten der chinesischen Bevölkerung und Unternehmen zu kontrollieren und zu verwalten.

Unter Präsident Xi Jinping wird die Informationstechnologie als politisches Instrument eingesetzt, um Gesetze und Vorschriften durchzusetzen und menschliches Verhalten an die von der Kommunistischen Partei Chinas (KPC) festgelegten gesellschaftlichen Normen mit dem Ziel anzupassen, eine zivilisierte Gesellschaft zu schaffen.¹¹⁸

3.1.4. Das Sozialkreditsystem (SKS)

Der Begriff *Kredit* (xinyong) im SKS (shehui xinyong tixi) hat im Chinesischen mehrere Definitionen. Er umfasst nicht nur Begriffe der finanziellen Fähigkeit, sondern ist auch mit Begriffen wie Aufrichtigkeit, Ehrlichkeit und Integrität verbunden.¹¹⁹ In 2007 veröffentlichte der Staatsrat von China einen Leitfaden für die Konstruktion des SKS, in dem der Sozialkredit als „...eine wichtige strukturelle Anordnung im marktwirtschaftlichen System...“ beschrieben wurde.¹²⁰ In diesem Leitfaden wird auch erwähnt, dass die Konzentration auf Perfektionierung der Kreditunterlagen in Bezug auf Kredite, Steuerzahlungen, Vertragserfüllung und Produktqualität liegt.¹²¹

¹¹⁴ Vgl. The Guardian (17.11.2020). Chinese City plans to turn Coronavirus App into permanent health tracker

¹¹⁵ Vgl. The Guardian (17.11.2020). Chinese City plans to turn Coronavirus App into permanent health tracker

¹¹⁶ Vgl. Liang, et al. (2018) S. 426

¹¹⁷ Vgl. Liang, et al. (2018) S. 426

¹¹⁸ Vgl. Meissner & Wübbecke (2016), S. 52

¹¹⁹ Vgl. Creemers (2018), S. 2

¹²⁰ Vgl. State Council General Office (20.11.2020). State Council General Office Some Opinions concerning the Construction of a Social Credit System

¹²¹ Vgl. State Council General Office (20.11.2020). State Council General Office Some Opinions concerning the Construction of a Social Credit System

Der Entwurf für den Aufbau des SKS wurde in 2014 vom Staatsrat veröffentlicht. In diesem Plan wird die Beschleunigung der Entwicklung des SKS, erstens, als eine „...wichtige Grundlage für die umfassende Umsetzung der wissenschaftlichen Entwicklungssicht und den Aufbau einer harmonischen sozialistischen Gesellschaft...“ beschrieben.¹²² Zweitens wird das SKS auch als eine wichtige Methode zur Beschleunigung und Verbesserung der sozialen Governance gesehen und drittens soll es eine große Bedeutung „...für die Stärkung des Aufrichtigkeitsbewusstseins der Gesellschaft, für die Schaffung eines wünschenswerten Kreditumfelds, für die Erhöhung der allgemeinen Wettbewerbsfähigkeit des Landes und für die Stimulierung der Entwicklung der Gesellschaft und des Fortschritts...“ haben.¹²³ Der Zeitraum für die vollständige Entwicklung umfasst 2014-2020. Die Einführung des SKS in 2020 wurde aufgrund der COVID-19-Pandemie verschoben, damit die Unternehmen, die in der Pandemie wirtschaftliche Schwierigkeiten erleben mussten, ihre Arbeit wieder aufnehmen und ihren gesetzlichen Verpflichtungen nachkommen können.¹²⁴ Aktuell wird das SKS in 21 chinesischen Städten auf kommunaler Ebene umgesetzt.¹²⁵

3.1.4.1. Datensammlung des SKS

Durch das Cybersicherheitsgesetz von 2016 werden die staatliche Kontrolle und der Datenzugang erleichtert, die eine Reihe von Anforderungen an Internetfirmen stellt.¹²⁶ Diese Internetfirmen haben auch Verantwortungen, wie Selbstzensuren, die unter Kapitel 3.1.1.1. *Das Prinzip der Great Firewall* genauer beschrieben werden. Auch wenn es keine offiziellen Berichte darüber gibt, woher China die Daten, mit denen die Bevölkerung bewertet werden soll, bekommen wird, gibt es bereits umgesetzte Überwachungssysteme, die durchaus im SKS eingesetzt werden könnten.

Videoüberwachung

Laut dem Industrieanalysten IHS Markit, wird in 2021 die Anzahl der Überwachungskameras in China 560 Millionen betragen, was China das meistüberwachte Land macht.¹²⁷ Das bedeutet, dass es etwa eine Überwachungskamera pro 2,5 Bürger geben wird. Die Videoüberwachung liefert die Grundlage für das Gesichtserkennungssystem.

¹²² Vgl. State Council General Office (20.11.2020). Planning Outline for the Construction of a Social Credit System (2014-2020)

¹²³ Vgl. State Council General Office (20.11.2020). Planning Outline for the Construction of a Social Credit System (2014-2020)

¹²⁴ Vgl. Trivium Social Credit (25.11.2020). Supreme People's Court grants leniency to support post-COVID work resumption

¹²⁵ Vgl. Chuncheng (2019), S. 26

¹²⁶ Vgl. Creemers, et al. (25.11.2020). Cyber Security Law 2016

¹²⁷ Vgl. IHS Markit (2019), S. 5

Gesichtserkennung und Künstliche Intelligenz

Gesichtserkennung und KI werden eingesetzt, um die durch Videoüberwachung erhobenen Beweise zu analysieren und zu verstehen, um Kriminelle zu verfolgen und verdächtiges Verhalten zu erkennen, um den Alltag der 1,4 Milliarden Menschen in China zu überwachen.¹²⁸ Diese Videobeweise werden schlussendlich in einer Datenbank mit anderen Daten zusammengefasst und mit dem Personalausweis und Gesicht jedes Einzelnen verknüpft.¹²⁹ In öffentlichen Bereichen wie U-Bahnstationen werden die Gesichter von Personen, die ihre Schulden nicht bezahlen, oder von Fußgängern, die bei Rot die Straße überqueren, angezeigt.¹³⁰

Behörden und Unternehmen

Zusätzlich zu den Videomaterialien, die von den Überwachungskameras und Gesichtserkennungssoftware aggregiert werden, sammeln Regierungsbehörden und private Unternehmen auch viele Daten, wie zum Beispiel zum finanziellen Status einer Person, Social-Media-Aktivitäten, Online-Einkäufe, Gesundheitsdaten, Steuererzahlungen oder rechtliche Angelegenheiten.¹³¹

Daten, die auf Nichteinhaltung gesetzlich vorgeschriebener sozialer und wirtschaftlicher Verpflichtungen hinweisen, werden, um die Vertrauenswürdigkeit von Unternehmen und Einzelpersonen zu ermitteln, gekennzeichnet. Das Ergebnis kann eine Bestrafung oder eine Belohnung sein. Der Weg zur Bestrafung bzw. Belohnung wird in der Abbildung 3 genauer dargestellt.

¹²⁸ Vgl. The Washington Post (25.11.2020). Beijing bets on facial recognition in a big drive for total surveillance

¹²⁹ Vgl. The Washington Post (25.11.2020). Beijing bets on facial recognition in a big drive for total surveillance

¹³⁰ Vgl. The New York Times (25.11.2020). Inside China's Dystopian Dreams: AI, Shame and Lots of Cameras

¹³¹ Vgl. Forbes (25.11.2020). Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids?

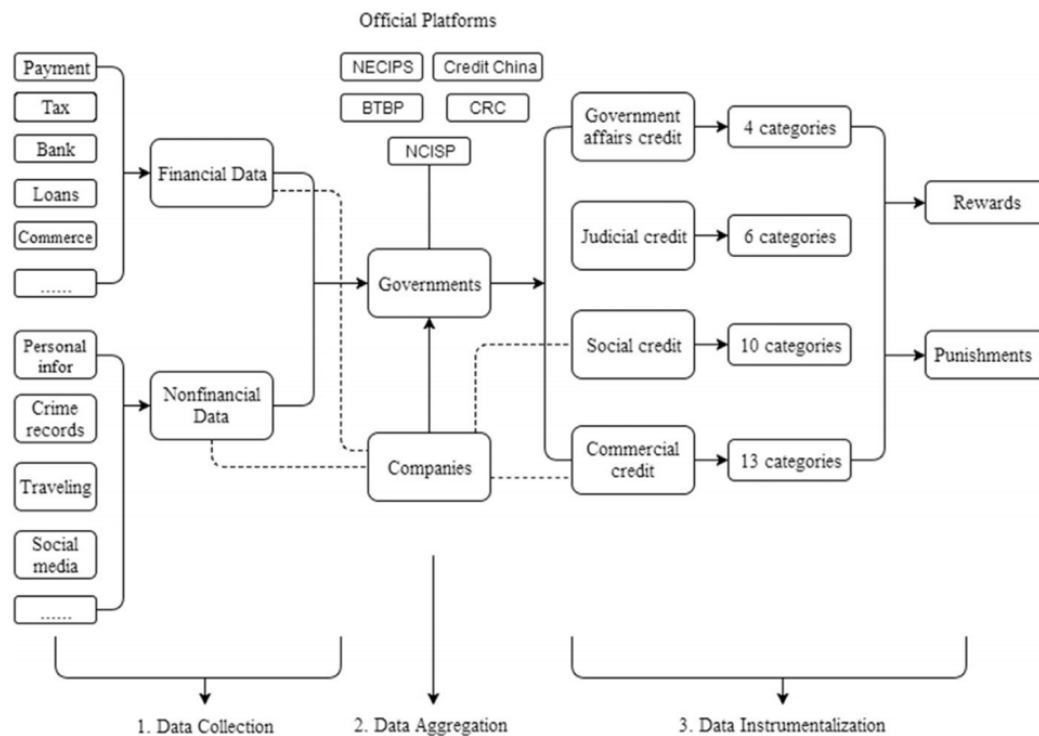


Abbildung 3: Datensammlung und Bestrafung¹³²

3.1.4.2. Das Bestrafungsmechanismus

Eine Bestrafung im SKS basiert auf ein sogenanntes Blacklist-System, in dem identifizierte Verbrecher in eine öffentliche Liste eingetragen werden, was für diese Personen bedeutet, dass sie für bestimmte Aktivitäten gesperrt werden.¹³³ Mehrere Institutionen und Regierungsbehörden führen eigene Blacklists von Unternehmen und Individuen, die von der NCISP gesammelt und analysiert werden.¹³⁴ Die analysierten Daten werden von NCISP an Credit China - eine weitere chinesische Datenplattform - weitergereicht, die schlussendlich die Blacklist veröffentlicht.¹³⁵ Die Eintragung in eine Blacklist kann erfolgen, wenn die Person bzw. Organisation die folgenden Fehlverhalten zeigen:

- Steuerhinterziehung,
- Nichtzahlung von Verwaltungsgebühren,
- Betrug im Geschäftsverkehr, Staatliche Prüfungen oder Anträge auf Sozialversicherung,
- Unfälle, die die Sicherheit der Öffentlichkeit, der Arbeit oder des Umweltschutzes betreffen,
- regierungskritische soziale Medienbeiträge,

¹³² Vgl. Liang, et al. (2018), S. 427

¹³³ Vgl. Creemers (2018), S. 13

¹³⁴ Vgl. Liang, et al. (2018), S. 433

¹³⁵ Vgl. Liang, et al. (2018), S. 433

- störendes Verhalten in öffentlichen Verkehrsmitteln,
- das Überqueren einer roten Ampel, etc.^{136 137}

Gutes Verhalten wiederum bringt eine Eintragung in die Redlist mit sich. Diese Liste umfasst Personen bzw. Organisationen, die folgende gute Verhalten zeigen:

- Leistung einer Freiwilligenarbeit,
- vorbildliche Steuerzahler,
- gute Arbeitsbeziehungen,
- geleisteter Beitrag zur Entwicklung des chinesischen Sozialismus,
- guter Kreditscore,
- aktive Teilnahme an sozialen Wohltätigkeitsorganisationen,
- Beitrag zum Umweltschutz, etc.¹³⁸

Privatpersonen, die in der Blacklist stehen, werden als „nicht qualifiziert“ für den Kauf eines Flugtickets, die Fahrt auf einigen Bahnlinien, den Kauf von Eigentum oder die Aufnahme eines Darlehens eingestuft.¹³⁹ Die juristischen Personen können hingegen mit Sanktionen, wie Einschränkung der Devisenquoten und des Zugangs zu Krediten und andere Finanzierungsmitteln, Verhindern von Einstieg in die Börse, keine Genehmigung für neue wissenschaftliche und technische Projekte oder verstärkte Inspektionen des Unternehmens, rechnen.¹⁴⁰

Die Redlist bringt eine Menge Vorteile für Individuen und für Organisationen mit sich. Eine Belohnung in dem Sinne für eine private Person wäre ermäßigte Energierechnungen, Verzicht auf Kauttionen für Mietobjekte, bessere Reiseangebote oder ein Arztbesuch ohne längere Wartezeiten.¹⁴¹ Für Unternehmen ergeben sich Vorteile, wie schnelle Abwicklung von Verwaltungsverfahren und Kreditzulassungen, Priorisierung für Auszeichnungen, vorrangige Beteiligung an Wirtschafts- und Handelsmessen und internationale Konferenzen oder Unterstützung des Unternehmens bei Rechtsberatung.¹⁴²

¹³⁶ Vgl. Chen & Cheung (2017), S. 16

¹³⁷ Vgl. Wired (30.11.2020). The complicated truth about China's social credit system

¹³⁸ Vgl. Schaefer & Yin (2019), S. 17ff

¹³⁹ Vgl. Wired (30.11.2020). The complicated truth about China's social credit system

¹⁴⁰ Vgl. Wired (30.11.2020). The complicated truth about China's social credit system

¹⁴¹ Vgl. Forbes (30.11.2020). Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steroids?

¹⁴² Vgl. Schaefer & Yin (2019), S. 19

3.2. Überwachung in Russland

Der russische digitale Autoritarismus ist gekennzeichnet durch eine allgegenwärtige Sammlung von Kommunikationsdaten, fehlende Aufsicht und die staatliche Einflussnahme auf die Industrie.¹⁴³ Obwohl Russlands digitaler Autoritarismus weder so gut definiert noch technologisch so robust oder auf künstliche Intelligenz angewiesen ist wie das chinesische Modell, ergreift die russische Regierung dennoch Maßnahmen, die die staatliche Überwachung weltweit fördern.¹⁴⁴

3.2.1. SORM – System für operative Ermittlungsaktionen

Die russische Regierung war bereits Ende der 1990er Jahre über die Auswirkungen des Informationsflusses innerhalb der Gesellschaft auf die nationale Sicherheit besorgt, was dazu führte, dass das Land ein neues Gesetz über operative Ermittlungen annahm, das dem Föderalen Sicherheitsdienst (FSB) die Befugnis übertragen hat, die gesamte private Kommunikation der Bürger, einschließlich der elektronischen Kommunikation, zu überwachen.¹⁴⁵ In 1995 wurde die erste Infrastruktur des „Systems für operative Ermittlungsaktivitäten“ (SORM) errichtet, die die Telefongespräche und E-Mail-Verkehr überwachte.¹⁴⁶ Einige Jahre später wurde dieses System erweitert (SORM-2), um auch die Überwachung des Internetverkehrs zu ermöglichen.¹⁴⁷ Eine weitere Erweiterung des Systems kam in 2012, die nun auch die Sozialen Medien überwacht.¹⁴⁸ Die letzte Version des Systems SORM-3 fängt jede Form der Kommunikation – inklusive Soziale Medien – und beinhaltet auch eine Langzeitspeicherung der Daten.¹⁴⁹ Nach russischem Recht müssen alle Internetdiensteanbieter *Punkt Upravlenia*, ein FSB-Überwachungsgerät, in ihren Netzwerken installieren, das den Datenverkehr ohne Wissen oder Zusammenarbeit des Diensteanbieters direkt aufzeichnen kann.¹⁵⁰ Die Sammlung von diesen Daten bzw. das Abhören von Personen erfordert einen Gerichtsbeschluss, der jedoch dem Internet Service Provider (ISP) bzw. Telekommunikationsanbieter nicht vorgelegt werden muss, um an die Daten zu kommen. Es reicht vom Gericht die Erlaubnis zum Abhören zu holen, und der FSB bekommt den Zugang zu SORM-Daten des ISPs bzw. Telekommunikationsanbieters.¹⁵¹ In den Winterolympiaden 2014 in Sotschi wurde das SORM-System verwendet, um Athleten, Trainer, Journalisten und Zuschauer

¹⁴³ Vgl. Morgus (2019), S. 91

¹⁴⁴ Vgl. Morgus (2019), S. 89

¹⁴⁵ Vgl. Kerr (2019), S. 64

¹⁴⁶ Vgl. Maréchal (2016), S. 33

¹⁴⁷ Vgl. Kerr (2019), S. 64

¹⁴⁸ Vgl. Maréchal (2016), S. 33

¹⁴⁹ Vgl. Reporters Without Borders (08.12.2020). Enemies of the Internet 2014 – Russia: Control from the top down

¹⁵⁰ Vgl. Lewis (08.12.2020). Reference Note on Russian Communications Surveillance

¹⁵¹ Vgl. Lewis (08.12.2020). Reference Note on Russian Communications Surveillance

zu überwachen, was mit dem Schutz vor Terrorismus begründet wurde.¹⁵² Den Geschäftsreisenden wurde geraten, um die Sicherheit der Kommunikationen sicherzustellen, „saubere“ Geräte zu verwenden und die Geräte nur dann zu verwenden, wenn sie wirklich benötigt werden.¹⁵³

3.2.2. Russland und China im Vergleich

Während der chinesische digitale Autoritarismus sehr techniklastig ist, basiert der russische Autoritarismus nicht auf Hochtechnologien. Die folgenden Punkte, machen das russische Modell verständlicher.¹⁵⁴

Das russische System ist auf eine Kombination aus Selbstzensur und Einschüchterung der Gesellschaft angewiesen, die durch komplexe, aber sehr restriktive Meinungsfreiheitsgesetze und eine offene Telekommunikationsüberwachung untermauert wird, als auf den Aufbau einer Internet-Infrastruktur zur Filterung massiver Inhaltsmengen.¹⁵⁵ Im Wesentlichen stützt sich das russische Modell auf das Gesetz, während Chinas digitaler Autoritarismus zur Durchsetzung seines autoritären Ansatzes zunehmend auf die Technologie setzt.¹⁵⁶

Weiteres produziert der russische Staat Informationen in hoher Menge und Geschwindigkeit. Diese Ressourcen werden für die interne Propaganda verwendet.¹⁵⁷ Das russische System versucht, den Informationsmarkt mit regierungsfreundlicher Propaganda zu überschwemmen und die negative Presse zu unterdrücken, statt das Informationsangebot im Internet eng zu begrenzen.¹⁵⁸

Letztlich mangelt es Russland an der für die chinesische Industrie charakteristischen industriellen Robustheit im Hochtechnologiebereich, was der russischen Industrie das Engagement auf den ausländischen Märkten verhindert, obwohl russische Überwachungsunternehmen nur begrenzt in autoritär geprägte Teile der Welt vordringen konnten.¹⁵⁹

¹⁵² Vgl. The Guardian (08.12.2020). Russia to monitor all communications at Winter Olympics in Sochi

¹⁵³ Vgl. The Guardian (08.12.2020). Russia to monitor all communications at Winter Olympics in Sochi

¹⁵⁴ Vgl. Morgus (2019), S. 89

¹⁵⁵ Vgl. Morgus (2019), S. 89ff

¹⁵⁶ Vgl. Morgus (2019), S. 90

¹⁵⁷ Vgl. Morgus (2019), S. 90

¹⁵⁸ Vgl. Morgus (2019), S. 90

¹⁵⁹ Vgl. Morgus (2019), S. 90

3.3. Überwachung in Europa

Durch die Enthüllungen von Edward Snowden, einem ehemaligen Mitarbeiter der US-amerikanischen National Security Agency (NSA), über die Aktivitäten der NSA, kam es ans Licht, dass die europäischen Dienste mit der NSA zusammenarbeiteten.¹⁶⁰ Diese Zusammenarbeit zwischen des britischen Geheimdienstes Government Communications Headquarters (GCHQ) und der NSA umfassten Abhöraktionen im Rahmen eines Programms mit dem Codenamen *TEMPORA*.¹⁶¹ Weiteres wurde auch bekannt, dass die EU-Mitgliedstaaten Schweden, Frankreich, Deutschland und die Niederlande ihre eigenen Abhörprogramme entwickeln und mit der NSA beim Austausch von Daten zusammenarbeiten.¹⁶²

3.3.1. Deutschlands BND-Spionageaffäre

Die Dokumente von Snowden zeigen, dass die NSA, die sich auf die Terrorismusbekämpfung und nationale Sicherheit konzentriert, auch mit dem deutschen Bundesnachrichtendienst (BND) ihre Überwachungssysteme geteilt hat, der damit digitale Daten gesammelt und jede Menge Kommunikationen der Bevölkerung überwacht hat.¹⁶³

Laut Spiegel wurden Daten aus Internetleitungen und Satellitenverbindungen gesammelt, in denen mit Selektoren nach Informationen gesucht wurden, welche von der NSA bestimmt wurden.¹⁶⁴ Beispiele für solche Suchbegriffe können IP-Adressen, Telefonnummern, E-Mail-Adressen oder auch Namen sein. Um zu vermeiden, dass die Daten der deutschen Bürger gesammelt werden, wurden aus den Selektoren die Länderkennung „+49“ und die Endung „.de“ von E-Mail-Adressen entfernt.¹⁶⁵ Die Datenbanken der BND sammelten alle Daten, die unter diesem Filter fielen, welche weiter an die NSA weitergereicht wurden. Neben den gefilterten Daten wurden auch Rohdaten wie ungefilterte Kommunikationen gesammelt. Wie Zeit Online berichtet, wurden von BND pro Tag 220 Millionen Metadaten abgehört, welche ohne eine inhaltliche Einsicht an die NSA geliefert wurden.¹⁶⁶ Im BND-Untersuchungsausschuss gaben auch BND-Mitarbeiter zu, dass diese Filter nicht immer funktionierten, sodass es möglich ist, dass auch Daten weitergereicht wurden, die gemäß dem Artikel 10-Gesetz¹⁶⁷ unter Schutz des Fernmeldegeheimnisses deutscher Bürger fallen.¹⁶⁸ Neben den klassischen Überwachungssystemen von

¹⁶⁰ Vgl. The Guardian (10.12.2020). NSA-Files decoded: What the revelations mean for you

¹⁶¹ Vgl. Bigo, et al., (2013), S. 9

¹⁶² Vgl. Bigo, et al., (2013), 39ff

¹⁶³ Vgl. Schaar (2015), S. 448

¹⁶⁴ Vgl. Spiegel (11.12.2020). Neue Spionageaffäre erschüttert BND

¹⁶⁵ Vgl. Spiegel (11.12.2020). So überwacht der BND das Internet

¹⁶⁶ Vgl. Zeit Online (11.12.2020). BND liefert NSA 1,3 Milliarden Metadaten – jeden Monat

¹⁶⁷ Vgl. Artikel 10-Gesetz (BGBl. I S. 1254, 2298, 2007 I S. 154)

¹⁶⁸ Vgl. Zeit Online (11.12.2020). BND liefert NSA 1,3 Milliarden Metadaten – jeden Monat

Russland und China, verwendet die NSA Metadaten, um an Informationen zu kommen. Auch diese Metadaten können viele Informationen zu einer Person liefern. Metadaten umfassen alles, was ein System über einen Datenverkehr wissen muss, um bei einer Abfrage die korrekten Daten geliefert werden.¹⁶⁹ Für eine digitale Kommunikation können diese Details zu dem Standort, den Benutzerdaten, der Geräteinfo oder der Dauer der Kommunikation sein. Zusammenfassend sind Metadaten eine Quelle, mit der ein Profil zu einem Menschen erstellt werden kann. Das hat der ehemalige Chef der NSA und CIA bestätigt, indem er in einer öffentlichen Diskussion gesagt hat: „*Wir töten Menschen auf Basis von Metadaten.*“¹⁷⁰

3.3.2. Das TEMPORA-Programm des britischen Geheimdiensts

Wie von The Guardian berichtet, hat das GCHQ ein Programm namens TEMPORA entwickelt, in dem Datenüberwachungsgeräte auf den Glasfaserkabeln platziert wurden, die die ein- und ausgehenden Internetdaten in Großbritannien transportieren und somit den Zugriff auf große Menge globalen Internetdaten dem GCHQ erlauben.¹⁷¹ Das GCHQ hat diese Daten bis zu 30 Tage lang gespeichert, um diese zu analysieren und zu sichten. Die Platzierung der Abhörgeräte auf den Glasfaserkabeln geschah mithilfe von kommerziellen Unternehmen, die in den NSA-Dokumenten als Abhörpartner bezeichnet wurden.

Die Legitimität der Operation wird jedoch angezweifelt. Laut dem Rechtsbeistand des GCHQ wurde ihr grünes Licht gegeben, indem altes Recht auf neue Technologie angewendet wurde. Regulation of Investigatory Powers Act (RIPA) aus dem Jahr 2000 schreibt vor, dass das Abhören definierter Ziele durch einen vom Innen- oder Außenminister unterzeichneten Haftbefehl genehmigt werden muss.¹⁷² Eine Klausel erlaubt es dem Außenminister jedoch, eine Bescheinigung für das Abhören vieler Materialien zu unterzeichnen, solange sich ein Ende der überwachten Kommunikation im Ausland befindet.^{173 174} Zu diesen Materialien gehörten bisher Betrug, Drogenhandel und Terrorismus, wobei die jeweiligen Kriterien geheim sind und keiner öffentlichen Diskussion unterliegen.

¹⁶⁹ Vgl. Gartner (2016), S. 2

¹⁷⁰ Vgl. Hayden (2014). Youtube

¹⁷¹ Vgl. The Guardian (12.12.2020). GCHQ taps fibre-optic cables for secret access to world's communications

¹⁷² Vgl. Art 41 Regulation of Investigatory Powers Act 2000 (RIPA)

¹⁷³ Vgl. Art 76A Regulation of Investigatory Powers Act 2000 (RIPA)

¹⁷⁴ Vgl. The Guardian (12.12.2020). GCHQ taps fibre-optic cables for secret access to world's communications

4. Politische Kampagnen und Big Data

Der vermehrte Einsatz von Big Data Analysen in politischen Kampagnen, um Profile von Wählerschaft zu erstellen und bestimmte Wählergruppen mit individualisierten Botschaften auf der Grundlage ihrer persönlichen Eigenschaften anzusprechen, wurde in den letzten Jahren Gegenstand einer intensiven Debatte. Mit politischem Microtargeting wird im modernen Wahlkampf versucht, Meinungen der Wählerschaft zu beeinflussen und bestimmte Wählergruppen von der Wahlurne fernzuhalten.

Dieses Kapitel untersucht den Datenskandal vom Analyseunternehmen Cambridge Analytica und Facebook im US-Wahlkampf von Donald Trump 2016 und im Brexit-Referendum 2016 und die Methoden, die in diesen politischen Kampagnen eingesetzt wurden.

4.1. Cambridge Analytica und Facebook-Datenskandal

The New York Times und The Observer enthüllten im März 2018, dass das Datenanalyseunternehmen Cambridge Analytica Daten von mehr als 50 Millionen Facebook-Profilen über eine Facebook-App erhalten hat, um Techniken zur Vorhersage und Manipulation des Verhaltens einzelner amerikanischer Wähler im US-Wahlkampf 2016 zu entwickeln.¹⁷⁵ Die Daten wurden über ein Persönlichkeitsquiz, das in der Facebook-App eingebunden war, gesammelt. Das Quiz wurde von rund 320.000 Nutzern heruntergeladen, die den Zugriff auf ihren persönlichen Daten und zusätzlich auf jene von ihren Facebook-Freunden erlaubt haben. Diese Personen waren sich jedoch nicht bewusst, dass ihre persönlichen Informationen gesammelt und kommerziell und möglicherweise auch politisch ausgenutzt wurden.

Cambridge Analytica war ein britisches Datenanalyse- und politisches Kommunikationsunternehmen, das 2014 von SCL Group (Strategic Communication Laboratories Group) unter der Leitung von Alexander Nix, gegründet wurde. Die SCL-Group wurde 1993 gegründet und hatte seitdem mehr als 200 Wahlen durchgeführt und in etwa 50 Ländern, wie Afghanistan, Kolumbien, Indien, Indonesien, Kenia, Kolumbien, Lettland, Libyen, Nigeria, Pakistan, die Philippinen, Trinidad und Tobago und mehr, Verteidigungs-, politische und humanitäre Projekte verwirklicht.¹⁷⁶

¹⁷⁵ Vgl. The New York Times (30.12.2020). How Trump Consultants Exploited the Facebook Data of Millions

¹⁷⁶ Vgl. Kaiser (2019), S. 10

„Wir haben uns auf das spezialisiert, was wir die Wissenschaft der Kommunikation von Verhaltensänderungen nennen. Das bedeutet, dass wir Verhaltensforschung, klinische und experimentelle Psychologie mit erstklassiger Datenanalyse kombiniert haben.“¹⁷⁷

Dieses Zitat stammt von Alexander Nix, der in einer Präsentation das Unternehmen vorgestellt hatte. Laut Brittany Kaiser, ehemalige Leiterin der Geschäftsentwicklung von Cambridge Analytica und Autorin des Buchs „Targeted“, beschäftigte Cambridge Analytica mehrere Psychologen und Data Scientists, die genau wussten, wen sie ansprechen wollten, welche Nachrichten diesen Personen zugesendet werden mussten und wo sie diese erreichen würden.¹⁷⁸ Dieses Team von Psychologen und Data Scientists konnte mit Hilfe von „Microtargeting“ Personen anvisieren und wusste genau, wo (am Computer, im Fernsehen) und wie (über Social Media, E-Mail, Telefon) diese Personen am besten erreicht werden konnten.¹⁷⁹ Die Aufgabe von Cambridge Analytica bestand darin, Einzelpersonen zu gruppieren bzw. zu isolieren und das Verhalten und die Gedankenweise dieser Personen zu ändern.

Kaiser erzählt in ihrem Buch „Targeted“ wie das Unternehmen die persönlichen Daten von Millionen von Menschen gesammelt hat und was sie genau mit diesen Daten gemacht haben.

4.2. Datenaggregation

Durch die immer stärkere Digitalisierung in allen Lebensbereichen werden mit jedem Klick im Internet, mit jeder Verwendung von Smart-Home-Geräten und Tablets bzw. Smartphones und mit jedem Schritt, der mit einem aktiven GPS-Tracker gemacht wird, Daten von Personen generiert und gesammelt. Für wichtige Analysen und Berechnungen von Erkenntnissen ist die Datenaggregation ein wichtiges Element.

Auch das Datenanalyseunternehmen Cambridge Analytica besaß eine enorme Menge an Daten und war auch in der Lage diese Menge zu vervielfachen. Neben der eigenen Datenbank, kaufte und lizenzierte Cambridge Analytica von verschiedenen Data Brokern (Unternehmen, die Informationen von verschiedenen Quellen sammeln, verarbeiten und bereinigen, um sie an andere Organisationen zu lizenzieren) wie Experian, Acxiom und Infogroup, Datensätze, die sie für die eigenen Analysen benötigten.^{180 181} Alleine für die Trump-Kampagne in den US-Wahlen

¹⁷⁷ Vgl. Kaiser (2019), S. 91

¹⁷⁸ Vgl. Kaiser (2019), S. 13

¹⁷⁹ Vgl. Kaiser (2019), S. 13

¹⁸⁰ Vgl. Kaiser (2019), S. 13

¹⁸¹ Vgl. Gartner (02.01.2021). Glossar – Data Broker

2016 besaß das Unternehmen zwischen 2.000 und 5.000 Data Points, welche jede mögliche persönliche Information über eine Person sind, von jedem bzw. jeder Amerikaner/Amerikanerin, der/die über 18 Jahre alt war, was damals etwa 240 Millionen Menschen entsprach.¹⁸² Sie kauften Daten über die finanzielle Situation der Amerikaner, wie zum Beispiel wo sie eingekauft haben, wieviel sie dafür bezahlt haben, wo sie Urlaub gemacht haben und vieles mehr.¹⁸³ Cambridge Analytica sammelte und aktualisierte ihre Daten laufend, um immer am aktuellsten Stand zu sein, welche Interessen die Menschen besaßen. Diese Menschen gaben ihre Daten preis, in dem sie „Cookies“ akzeptierten oder den Nutzungsbedingungen von Anwendungen zustimmten.¹⁸⁴ Jeder digitaler Fußabdruck von Internetnutzern wurden gesammelt und gespeichert, wenn nicht von Cambridge Analytica, dann von anderen Datenvermittlern, die mit diesen Informationen handeln. Ein anderer Weg an Daten zu kommen, den das Unternehmen oft verwendet hat, war, die eigenen Datenbanken gegen andere Datenbanken von Kunden bereitzustellen.¹⁸⁵ Es wurden auch Vereinbarungen geschlossen zur gemeinsamen Nutzung von Daten, die von den Kunden selbst produziert und auf dem freien Markt nicht verkauft wurden.

Eine der wichtigsten Quellen für die Datenerhebung war Facebook. Mit unterschiedlichsten Methoden konnten über Facebook hunderte Data Points über eine Person erhoben werden.

4.2.1. Datenermittlung über Facebook und die Friends API

Facebook war und ist eine wichtige Ressource für Daten von Einzelpersonen für Analysefirmen wie Cambridge Analytica. Der Datenmissbrauch von Facebook umfasste über 50 Millionen Facebook-Profilen, deren persönlichen Informationen ohne deren Erlaubnis von Cambridge Analytica für den Wahlkampf von Trump in den US-Wahlen 2016 ausgenutzt wurden.¹⁸⁶ Mittels Facebook konnte Cambridge Analytica etwa 570 individuelle Data Points über die Nutzer erheben, die sie mit anderen ermittelten Daten kombinierten und insgesamt etwa 5.000 Data Points über jeden einzelnen Amerikaner über 18 Jahren sammelten.¹⁸⁷

Die Data Scientists entwickelten verschiedene Persönlichkeitsquiz wie „The Sex Compass“ und „The Musical Walrus“ mit denen sie Data Points über die sexuelle und musikalische Persönlichkeit der Nutzer ermittelten.¹⁸⁸ Die Debatte um den Datenmissbrauch von Facebook brach jedoch um das Persönlichkeitsquiz „thisisyour-digitallife“ aus, das von Forscher Dr. Aleksandr Kogan und seinem Unternehmen

¹⁸² Vgl. Kaiser (2019), S. 12ff

¹⁸³ Vgl. Kaiser (2019), S. 77ff

¹⁸⁴ Vgl. Kaiser (2019), S. 78ff

¹⁸⁵ Vgl. Kaiser (2019), S. 82ff

¹⁸⁶ Vgl. The New York Times (30.12.2020). How Trump Consultants Exploited the Facebook Data of Millions

¹⁸⁷ Vgl. Kaiser (2019), S. 77ff

¹⁸⁸ Vgl. Kaiser (2019), S. 78ff

Global Science Research (GSR) entwickelt wurde. Laut dem Bericht von Information Commissioner's Office (ICO), eine britische Datenschutzbehörde, die den Datenskandal von Cambridge Analytica und Facebook untersuchte, entwickelte Dr. Kogan eine App, die er nach seinen eigenen Angaben ursprünglich im Rahmen seiner akademischen Forschung verwenden wollte, jedoch später über sein Unternehmen GSR für die kommerzielle Nutzung, Änderungen in der App durchführte.¹⁸⁹ Die App enthielt einen Persönlichkeitstest, den Dr. Kogan an Cambridge Analytica verkaufte, um persönliche Informationen von US-Bürgern für die Präsidentschaftswahlen zu sammeln.¹⁹⁰ Mit diesem Persönlichkeitstest konnten Dr. Kogan und CA bis zu 320.000 Nutzern in den USA erreichen.¹⁹¹ Zusätzlich zu den Antworten, die sie durch den Test gesammelt haben, nutzte die App die Anmeldung über Facebook, um die Einwilligung von Nutzern zu erhalten und auf bestimmte Daten aus dem Facebook-Profil zuzugreifen.¹⁹² Nach dieser Erlaubnis hatten Dr. Kogan und das Team auf die folgenden Arten von Informationen von Benutzern in gewissem Ausmaß Zugriff, je nachdem, welche Privatsphäre-Einstellungen diese in ihren Facebook-Profilen vorgenommen hatten:

- Fotos, auf denen die Benutzer markiert waren,
- Seiten, die von den Benutzern „geliked“ wurden
- eigene Beiträge und Beiträge von den Freunden in den Feeds der Benutzer,
- Freundeslisten,
- E-Mail-Adressen und
- Facebook-Nachrichten.¹⁹³

Die App holte außerdem noch die Erlaubnis, auf die folgenden Arten von Informationen von ihren Facebook-Freunden zuzugreifen:

- öffentliche Daten auf dem Profil,
- Geburtsdatum,
- aktueller Wohnort,
- Fotos, auf denen die Freunde markiert waren,
- Seiten, die von den Freunden „geliked“ wurden.¹⁹⁴

Somit konnten sie auf die persönlichen Daten von insgesamt 87 Millionen Facebook-Nutzer zugreifen, inklusive 1 Million britische Nutzer.^{195 196} Im Anhang A ist eine Zusammenfassung zur Datenerfassung von Facebook-Daten zu finden.

¹⁸⁹ Vgl. ICO (2018), S. 18ff

¹⁹⁰ Vgl. ICO (2018), S. 18ff

¹⁹¹ Vgl. ICO (2018), S. 19

¹⁹² Vgl. ICO (2018), S. 19

¹⁹³ Vgl. ICO (2018), S. 19ff

¹⁹⁴ Vgl. ICO (2018), S. 20

¹⁹⁵ Vgl. ICO (2018), S. 20

¹⁹⁶ Vgl. ICO (2018), S. 16

4.3. Politisches Microtargeting

Der Begriff „Microtargeting“ beschreibt den Prozess, in dem verschiedene Techniken angewandt werden, um die spezifischen Interessen von Einzelpersonen zu identifizieren und relevante oder personalisierte Botschaften für diese Personen zu erstellen, die Wirkung dieser Botschaften vorherzusagen und diese Botschaften direkt an diese gezielten Personen zu übermitteln.¹⁹⁷ Es werden Profile von Personen erstellt, die nach ihren Interessen und Eigenschaften segmentiert werden.¹⁹⁸ Mittels statistischen Analysetechniken kann zukünftiges Verhalten von Personen vorhergesagt werden. Im Falle von Wahlen wollte zum Beispiel Cambridge Analytica, dass die Menschen Geld spenden, sich über ihren Kandidaten informieren, in die Wahlkabinen gehen und für ihren Kandidaten stimmen.¹⁹⁹ Das Unternehmen nannte dieses Verfahren „Behavioral Microtargeting“ (Verhaltens-Microtargeting).²⁰⁰

4.3.1. OCEAN-Scoring

Cambridge Analytica verfügte neben der riesigen Datenbank ein Verfahren zur Persönlichkeitsanalyse namens OCEAN-Scoring, womit sie an Millionen von Menschen OCEAN-Scores vergaben.²⁰¹ Dieses Verfahren wurde in den 1980er von zwei Psychologen entwickelt und ermöglichte die Bestimmung der Konstruktion der Persönlichkeiten von Menschen.²⁰²

Das Modell identifizierte Persönlichkeitsmerkmale, die auf Offenheit (Openness - O), Gewissenhaftigkeit (Conscientiousness – C), Extravertiertheit (Extroversion - E), Verträglichkeit (Agreeableness – A) und Neurotizismus (Neuroticism – N) basieren.²⁰³ Mit den Daten, die über das Persönlichkeitsquiz gesammelt wurden, konnten sie die OCEAN-Scores von den Teilnehmern berechnen und diese Scores mit anderen Daten abgleichen.²⁰⁴ Mittels diesen zusammengefassten Daten konnten sie Eigenschaften und Merkmale sowie ethnische Zugehörigkeit und politische Einstellung mit hoher Genauigkeit vorhersagen.²⁰⁵ Personen, die aufgrund weniger persönlichen Informationen keiner Gruppe zugeordnet werden konnten, wurden mit anderen Personen verglichen, die ähnliche OCEAN-Scores nachwiesen, und dementsprechend gruppiert.²⁰⁶

¹⁹⁷ Vgl. ICO (2018), S. 27ff

¹⁹⁸ Vgl. ICO (2018), S. 27ff

¹⁹⁹ Vgl. Kaiser (2019), S. 83ff

²⁰⁰ Vgl. Kaiser (2019), S. 83ff

²⁰¹ Vgl. Kaiser (2019), S. 84

²⁰² Vgl. ICO (2018), S. 18

²⁰³ Vgl. ICO (2018), S. 18

²⁰⁴ Vgl. ICO (2018), S. 18

²⁰⁵ Vgl. ICO (2018), S. 18

²⁰⁶ Vgl. Kaiser (2019), S. 84ff

- **Offenheit**

Hier gibt der Wert für Offenheit die Aufgeschlossenheit der Person gegenüber neuen Erfahrungen an.²⁰⁷

- **Gewissenhaftigkeit**

Gewissenhafte Menschen sind organisiert und haben mehr Plan als Spontaneität im Leben.²⁰⁸

- **Extravertiertheit**

Die Eigenschaft Extravertiertheit einer Person zeigt, ob eine Person viele Menschen um sich hat und ein Teil der Gesellschaft ist.²⁰⁹

- **Verträglichkeit**

Der Wert zur Verträglichkeit einer Person sagt aus, wie freundlich die Person gegenüber ihren Mitmenschen ist.²¹⁰

- **Neurotizismus**

Neurotizismus gibt an, wie sehr die Person bei Entscheidungen von Angst getrieben ist.²¹¹

Diese Eigenschaften wurden danach noch mehr verfeinert, in dem sie die Themen noch hinzufügten, für die die Personen bereits Interesse, wie zum Beispiel durch Facebook-Likes, gezeigt hatten.²¹² Anschließend wurden Kampagnen auf Basis von Inhalten entworfen, die Cambridge Analytica mittels verschiedener Techniken generiert hatte. Somit wurden Millionen von Menschen segmentiert und für die Microtargeting-Strategie bereitgestellt.

Die Microtargeting-Strategie umfasste das Übermitteln der richtigen Botschaften als Video, Audio oder Printanzeigen an identifizierten Zielen. Oft mussten von 20 bis 30 Variationen derselben Anzeige an dieselbe Person geschickt und an verschiedenen Stellen ihres Social Media-Feeds platziert werden, bis die Person die Anzeige wahrgenommen und angeklickt hat.²¹³

²⁰⁷ Vgl. Laux (2008), S. 177

²⁰⁸ Vgl. Laux (2008), S. 177

²⁰⁹ Vgl. Laux (2008), S. 177

²¹⁰ Vgl. Laux (2008), S. 177

²¹¹ Vgl. Laux (2008), S. 177

²¹² Vgl. Kaiser (2019), S. 85ff

²¹³ Vgl. Kaiser (2019), S. 87ff

4.4. Rechtliche Konsequenzen

Nach Beginn der Durchsuchungen des Datenanalyseunternehmens Cambridge Analytica in 2018, meldete das SCL Group, die Muttergesellschaft von Cambridge Analytica, Insolvenz an.²¹⁴ Sowohl SCL Group als auch Cambridge Analytica mussten nach der Veröffentlichung des Datenskandals schließen.

Die amerikanische Verbraucherschutzbehörde Federal Trade Commission (FTC) kam mit Facebook in 2019 zu einem Vergleich, in dem sie Facebook wegen Datenschutzverletzung eine Strafe von 5 Milliarden Dollar verhängt hat.²¹⁵ In einem Pressebericht erklärte das FTC, dass Facebook gegen eine Verordnung des FTC aus dem Jahr 2012 verstoßen hat, indem es die Nutzer über ihre Möglichkeiten zur Kontrolle der Privatsphäre ihrer persönlichen Daten getäuscht hat.²¹⁶ FTC geht davon aus, dass viele Nutzer nicht wussten, dass Facebook persönliche Informationen auch von Facebook-Freunden, über Apps von Drittanbietern weitergab, und daher die Einstellungen zur Privatsphäre nicht angepasst haben können.²¹⁷ Die neue Verordnung beschränkt weiteres die Geschäftstätigkeit von Facebook und sieht eine Rechenschaftspflicht in Bezug auf Datenschutz auf die Vorstandsebene vor.²¹⁸ Sie schafft ein unabhängiges Datenschutz-Komitee des Vorstands von Facebook, das die uneingeschränkte Kontrolle von Facebooks CEO Mark Zuckerberg über Entscheidungen, die die Privatsphäre der Nutzer betreffen, verhindert.²¹⁹

Die Untersuchung von ICO weist ebenfalls darauf hin, dass die Einwilligung der Facebook-Nutzer nicht ausreichend informativ ist, vor allem in Bezug auf die Daten der Freunde und die Art und Weise, wo diese Daten genutzt und zu welchem Zweck diese an Dritte weiterverkauft werden könnten.²²⁰ Das ICO verhängte Facebook eine Strafe in Höhe von 500.000 Pfund aufgrund ungerechtfertigter Nutzung von persönlichen Daten von Facebook-Nutzern.²²¹

Das ICO hat im Oktober 2020 die Untersuchung zur Nutzung von persönlichen Daten und politischer Einflussnahme von Cambridge Analytica abgeschlossen. Die Chefin der britischen Datenschutzbehörde ICO Elizabeth Denham berichtete in

²¹⁴ Vgl. The Guardian (05.01.2021). Cambridge Analytica closing after Facebook data harvesting scandal

²¹⁵ Vgl. FTC (05.01.2021). FTC imposes 5\$ Billion Penalty and Sweeping New Privacy Restrictions on Facebook

²¹⁶ Vgl. FTC (05.01.2021). FTC imposes 5\$ Billion Penalty and Sweeping New Privacy Restrictions on Facebook

²¹⁷ Vgl. FTC (05.01.2021). FTC imposes 5\$ Billion Penalty and Sweeping New Privacy Restrictions on Facebook

²¹⁸ Vgl. FTC (05.01.2021). FTC imposes 5\$ Billion Penalty and Sweeping New Privacy Restrictions on Facebook

²¹⁹ Vgl. FTC (05.01.2021). FTC imposes 5\$ Billion Penalty and Sweeping New Privacy Restrictions on Facebook

²²⁰ Vgl. ICO (2018), S. 21

²²¹ Vgl. Denham (2020)

ihrem Brief an einen parlamentarischen Ausschuss, dass das ICO keine Beweise dazu gefunden hat, dass Cambridge Analytica in das EU-Referendum 2016 involviert war.²²² Außerdem bestätigte Denham in ihrem Brief das Vorhandensein der Facebook-Daten und die sichere Löschung dieser von allen möglichen Servern.²²³

²²² Vgl. Denham (2020)

²²³ Vgl. Denham (2020)

5. Gefahren von Big Data

Viele Menschen sehen Big Data als eine große Chance für die Menschheit. Andere verzweifeln aber auch um die großen Risiken, die Big Data mit sich bringt. Big Data hat mittlerweile in vielen Bereichen Einsatz. Welche Risiken kann Big Data für Unternehmen und Privatpersonen haben und welche Kompromisse müssen eingegangen werden?

Unternehmen sammeln mittels verschiedener Techniken für verschiedene Zwecke eine immense Menge an Daten von ihren Kunden. Wie im Kapitel 3 beschrieben, sammeln auch Regierungen Daten von ihren Bürgern. China ist am Weg, mit einem Sozialkreditsystem seiner Bevölkerung Sozialkredite zu vergeben und somit seine Bevölkerung zu kontrollieren. Viele Länder sammeln mittlerweile viele personenbezogene Daten von ihren Bürgern, meistens wird die Datensammlung mit Terrordrohungen begründet. Mit KI-Systemen, die mit diesen Daten gefüttert werden, können Regierungen ihre Bürger beobachten und sehen, wie sich diese Bürger verhalten. Unternehmen verwenden Big Data, um zu lernen, welche Produkte ihre Kunden mehr ansprechen könnten und um später mit gezieltem Marketing ihre Produkte zu werben. Das Kapitel 4 zeigt, wie politische Parteien Big Data anwenden, um potentielle Wähler mit direkten Botschaften anzusprechen und mehr Vertrauen zu bilden.

Dieses Kapitel erläutert die Risiken von Big Data sowohl für die Unternehmen und Gesellschaft als auch für die Demokratie.

5.1. Manipulation

Maschinen lernen, Menschen zu programmieren.²²⁴ Menschen bekommen meistens nicht mit, dass sie ein Ziel von einem Unternehmen oder von politischen Kampagnen werden, wenn sie eine Werbung oder Botschaft zu sehen bekommen, die genau ihren Wünschen entspricht. Entscheidungen, die aufgrund dieser gezielten Werbungen oder Botschaften getroffen werden, wird in Wirklichkeit oft von anderen entschieden und von der Zielperson aufgezwungen.²²⁵ Politische Kampagnen können mit personalisierten Botschaften die Meinungen der Bürger manipulieren und somit sogar Wahlergebnisse beeinflussen.

Mit einem Einkauf eines Buches werden Daten generiert, die von Verkäufern gespeichert werden, und später dafür verwendet werden, um ein Profil von Vorlieben des Kunden zu erstellen. Durch dieses Profil können Unternehmen mit gezielten persönlichen Werbungen die Kunden dazu bringen, nochmals von ihren Produkten

²²⁴ Vgl. Helbing (2019), S. 28

²²⁵ Vgl. Helbing (2019), S. 28

zu kaufen. Mit diesem Ansatz versuchen Unternehmen zu verstehen, welche Produkte ein Kunde, der beispielsweise ein Science-Fiction-Buch gekauft hat, noch bevorzugt, da sie somit auch anderen Kunden diese Produkte vorschlagen können, die auch dasselbe Buch gekauft haben. Die Onlineshops werben für diese Produkte unter Titeln, wie „Das könnte Sie noch interessieren“ oder „Kunden, die dieses Produkt gekauft haben, haben auch diese Produkte dazu bestellt“. Eine Person, die gerade ein Buch bestellt hat, kann Werbeanzeigen von Buchstützen bekommen, weil eine andere Person, die auch das Buch bestellt hatte, noch zusätzlich eine Buchstütze gekauft hatte. Auch wenn diese Person gar nicht den Gedanken hatte, eine Buchstütze zu kaufen, wird mit dieser Werbeanzeige versucht, den Wunsch in dieser Person zu erwecken, welche zu kaufen. Somit werden die Entscheidungen und das Verhalten der Kunden beeinflusst bzw. manipuliert.

5.2. Massenüberwachung

China will mit dem Sozialkreditsystem seine Bürger kontrollieren, um Verbrechen und ungewolltes Verhalten der Bürger zu vermeiden. Mit dem Sozialkreditsystem werden die Bürger kategorisiert und Entscheidungen werden nach dem Sozialkredit der Bürger getroffen. Wer einen höheren Kredit hat, wird bei den Entscheidungen bevorzugt. Ein solcher Ansatz ist mit den demokratischen Grundprinzipien und -rechte nicht vergleichbar.²²⁶ Es wäre eine große Gefahr für die Demokratie, wenn dieses chinesische Modell in anderen Ländern zur Anwendung kommen würde.²²⁷ Trotz der beeindruckenden wirtschaftlichen Entwicklung Chinas ist es zu beachten, dass die durchschnittliche Lebensqualität der Volksrepublik China weit niedriger ist als in den demokratischen Staaten.²²⁸

Das größte Problem stellen die Länder dar, die einen Zugang zu Big Data Infrastrukturen haben. Zu diesen Problemländern zählen auch jene, die ein Ziel des Terrors sind, denn Terroranschläge oder andere traumatische Ereignisse können dazu genutzt werden, um demokratische Prinzipien einzuschränken.²²⁹ In Frankreich wurde 2017 ein neues Anti-Terror-Gesetz beschlossen, das die Maßnahmen des Ausnahmezustandes nach den Terroranschlägen in Paris ins Recht übernommen hat und somit den Sicherheitsbehörden erweiterte Befugnisse verschafft.²³⁰ Ähnliche Entwicklungen gibt es auch in Polen, Ungarn und in der Türkei, die durch Verfassungsänderungen sich mehr Freiheit zur Überwachung schaffen und die

²²⁶ Vgl. Helbing (2019), S. 28

²²⁷ Vgl. Helbing (2019), S. 28

²²⁸ Vgl. Statista (20.01.2021). Ranking der 20 Länder mit der höchsten Lebensqualität nach dem Best Countries Ranking 2020

²²⁹ Vgl. Helbing (2019), S. 28

²³⁰ Vgl. Zeit Online (15.01.2021). Neues Anti-Terror-Gesetz statt Ausnahmezustand

Opposition unterdrücken.²³¹ Das Beispiel China zeigt, wie sie durch Gesetze die Unternehmen dazu zwingen, alle möglichen Daten von Kunden zu speichern und mit der Regierung zu teilen, wie im Kapitel 3 beschrieben.

5.3. Die große Macht der Technologieunternehmen

Ein Vorfall, der sich im Jänner 2021 vor dem Ende der Amtszeit von Donald Trump als Präsident der Vereinigten Staaten ereignete, zeigt die Macht der Technologieunternehmen in einer digitalisierten Gesellschaft. Am 7. Jänner 2021, als sich der Senat und das Repräsentantenhaus im Kapitol in Washington sammelten, um das Ergebnis der Präsidentschaftswahl festzustellen, stürmten Trump-Anhänger das Kapitol. Bei diesen Ausschreitungen kamen fünf Menschen ums Leben. Als Auslöser dieser Ausschreitungen werden die Tweets und Aussagen von Donald Trump gesehen, in denen er mehrmals behauptete, dass der Wahlsieg gestohlen sei und er das Wahlergebnis nicht anerkennen werde.

Bereits in der Nacht der Ausschreitungen wurde das Twitter-Konto von Donald Trump für 12 Stunden gesperrt und drei Tweets, die zufolge der Ausschreitungen in Washington von Trump gepostet wurden, gemäß der Richtlinie der bürgerlichen Integrität von Twitter, gelöscht.²³² ²³³ Ein Tag später verkündete Twitter mit einem Blog-Post die permanente Suspendierung von Trumps Twitter-Konto.²³⁴ In dem Blog wurde als Grund der Suspendierung das Bestehen des Risikos der weiteren Anstiftung zur Gewalt angegeben.²³⁵ Facebook reagierte ähnlich und sperrte das Facebook- und Instagram-Konto von Trump für eine unbestimmte Zeit auch mit der Begründung, dass die Risiken, die mit der weiteren Nutzung der Dienste von Facebook durch Präsident Trump verbunden sind, zu groß sind.²³⁶ Die Reaktion auf die Entscheidung von Social-Media-Plattformen aus dem politischen Spektrum war sehr unterschiedlich. Manche waren erfreut darüber, dass die Online-Präsenz von Trump von den Social-Media-Unternehmen kontrolliert wurde. Andere hingegen sahen diese Aktionen als eine Erosion der Meinungsfreiheit.²³⁷

Fragen wie, ob die Geschäftsmodelle der Social-Media-Unternehmen mit einer Demokratie vereinbar sind und wie viel Einfluss die sozialen Medien auf die politischen Entscheidungen der Gesellschaft hat, wurden wiederum nach diesen Aktionen

²³¹ Vgl. Helbing (2019), S. 29

²³² Vgl. Twitter (31.01.2021). Twitter Safety

²³³ Vgl. Twitter (31.01.2021). Civic Integrity Policy

²³⁴ Vgl. Twitter (31.01.2021). Permanent Suspicion of @realDonaldTrump

²³⁵ Vgl. Twitter (31.01.2021). Permanent Suspicion of @realDonaldTrump

²³⁶ Vgl. Facebook (31.01.2021). Our Response to the Violence in Washington

²³⁷ Vgl. The Guardian (31.01.2021). Should we celebrate Trump's Twitter ban? Five free speech experts weigh in

aufgeworfen.²³⁸ Die Sozialen Medien bringen verschiedene Arten von Manipulationsmöglichkeiten mit sich.²³⁹ Soziale Medien können dazu verwendet werden, um das Volk zu verhetzen oder Hass zu verbreiten. Andererseits ermöglichen, die aus den sozialen Medien gesammelten Daten, die Manipulation der Menschen, sei es die Manipulation der politischen Meinungsbildung oder einer Meinungsbildung zu einem anderen Thema.

5.4. Probleme der Big Data Analytics

Neben den zahlreichen Erleichterungen, die Big Data Lösungen mit sich bringen, gibt es auch einige Problembereiche dieser Technologien, die beachtet werden müssen. Diese Probleme werden in den folgenden Abschnitten geschildert.

Diskriminierung

Die, mithilfe von Big Data Analytics gewonnenen Erkenntnisse können manchmal zu Entscheidungen führen, die Menschen diskriminieren und damit gegen die Verfassung oder das Gesetz verstoßen. Eine Studie zeigt, dass Google seinen weiblichen Nutzern weniger gut bezahlte Jobanzeigen anzeigt als seinen männlichen Nutzern.²⁴⁰ Eine weitere Studie der Harvard University zeigt eine statistisch signifikante Diskriminierung bei den Anzeigen von Google-Suchen nach rassistisch assoziierten Namen.²⁴¹ Die Wahrscheinlichkeit, dass eine Suche nach einem afroamerikanischen Namen, wie zum Beispiel Latanya, eine Anzeige für Verhaftungen lieferte, war um 25 Prozent höher als die Wahrscheinlichkeit bei einer Suche nach einem nicht-afroamerikanischen Namen, wie zum Beispiel Kristen.²⁴²

Mangelnde Sicherheit

Die angezeigten Fälle der Cyberkriminalität in Österreich hat sich von 2009 bis 2019 fast verdreifacht.²⁴³ In der COVID-19-Pandemie betrug der Schaden durch die Cyberkriminalität weltweit mehr als eine Billion Dollar.²⁴⁴ Die Cyberkriminalität umfasst Daten- und Identitätsdiebstahl, welche auch Big Data betreffen. Die Unternehmen müssen viele Maßnahmen ergreifen, um den Schutz der Daten sicherzustellen. Bei

²³⁸ Vgl. The New York Times (31.01.2021). In Pulling Trump's Megaphone, Twitter Shows Where Power Now Lies

²³⁹ Vgl. BMVIT (2017), S. 17

²⁴⁰ Vgl. Datta, et al., (2015), S. 92

²⁴¹ Vgl. Sweeney (2013), S. 4

²⁴² Vgl. Sweeney (2013), S. 34

²⁴³ Vgl. Statista (31.01.2021). Angezeigte Fälle von Cybercrime (gesamt) in Österreich von 2004 bis 2019

²⁴⁴ Vgl. Kurier (31.01.2021). Mehr als eine Billion Dollar Schaden durch Cyberkriminalität

Hackerangriffen und Datendiebstahl stellen besonders die zentral gespeicherten Datensammlungen eine große Gefahr dar.²⁴⁵

Objektivität

Die Erkenntnisse von Big Data Analysen werden oft als objektiv angesehen. Das stellt ein großes Problem dar, denn die Effektivität von Big Data mehr auf Überzeugungen basieren kann als auf Fakten. Es ist beispielsweise nicht bewiesen, dass Überwachungskameras die organisierte Kriminalität reduzieren können oder die Massenüberwachung bei der Terrorismusbekämpfung effektiver ist als die klassischen Ermittlungsmethoden.²⁴⁶ Vorhersagen können sich oft als fehlerhaft herausstellen und ein Grund dafür ist der Einfluss auf Nutzerverhalten durch personalisierte Anzeigen.²⁴⁷ Dieser Einfluss führt zu Veränderungen im Nutzerverhalten und diese Veränderung führt wiederum zu fehlerhaften Prognosen. Aus diesen Gründen sind die Schlussfolgerungen aus Big Data nicht immer zuverlässig.

Datenschutz

Die Grundidee von Big Data ist es mittels Data Mining aus dem Datenbestand neue Erkenntnisse zu gewinnen, die zur besseren Entscheidungsfindung oder als Grundlage für verbesserte Funktionen für den Kunden verwendet werden können.²⁴⁸ Diese Daten bestehen meistens aus persönlichen Merkmalen von Personen, was jedoch in Konflikt mit dem Datenschutz steht. Die datenbasierte Auswertung mittels Big Data Analysen kann es ermöglichen personenbezogene Merkmale aus bereits anonymen Datenbeständen abzuleiten.²⁴⁹ Es ist auch festzuhalten, dass je höher der Informationsgehalt der Daten ist, umso präziser die Ergebnisse einer Big Data Analyse sind, was auch bedeutet, dass durch die Anonymisierung die Qualität der Ergebnisse der Big Data Analysen immer geringer wird.²⁵⁰

²⁴⁵ Vgl. BMVIT (2017), S. 16

²⁴⁶ Vgl. Helbing (2019), S. 55ff

²⁴⁷ Vgl. Helbing (2019), S. 55ff

²⁴⁸ Vgl. BMVIT (2017), S. 16

²⁴⁹ Vgl. BMVIT (2017), S. 16

²⁵⁰ Vgl. BMVIT (2017), S.107

6. Rechtliche Herausforderungen

“Privacy is not something that I’m merely entitled to, it’s an absolute prerequisite.” – Marlon Brando

Die Digitalisierung erschwert die Wahrung der Privatsphäre und den Schutz der Daten. Auch in der Ära der Big Data und Big Data-Technologien wirft vor allem die Datensammlung und -verarbeitung Rechtsfragen für die Gesellschaft auf.

Dieses Kapitel setzt sich mit dem Datenschutzrecht auseinander. Es werden einzelne Regelungen der DSGVO und des österreichischen Datenschutzgesetzes näher untersucht.

In Österreich regelt die europäische Datenschutzgrundverordnung (DSGVO) und das Datenschutzgesetz (DSG) den Schutz der Daten. Die DSGVO aus dem Jahr 2018 reguliert die Digitalisierung, indem sie die personenbezogenen Daten natürlicher Personen bei der Erfassung, Speicherung und Verarbeitung schützt.²⁵¹ In Österreich wird die DSGVO um das DSG ergänzt.²⁵²

6.1. Europäische Datenschutzgrundverordnung (DSGVO)

Die Europäische Union hat in 2018 die weitreichende Datenschutzgrundverordnung (DSGVO) erlassen.²⁵³ Diese Verordnung garantiert EU-Bürgern und Einwohnern Schutz von ihren persönlichen Daten und erfordert ihre Zustimmung zu deren kommerzieller oder sonstiger Nutzung durch Dritte.²⁵⁴ Die Umsetzung der DSGVO in den Unternehmen stellte eine Herausforderung dar. Facebook hat vor dem Inkrafttreten der DSGVO im Mai 2018 1,5 Milliarden Nutzerprofile von Irland in den USA verschoben, um die DSGVO zu umgehen, denn im Gegensatz zur EU sieht die USA kein ausdrückliches Recht auf Daten- und Informationenschutz vor.²⁵⁵

Die DSGVO hat die alte europäische Datenschutzrichtlinie außer Kraft gesetzt, die das Ziel hatte, europäische Datenschutzstandards auf dasselbe Niveau zu bringen, jedoch entwickelten die Mitgliedstaaten mit der Zeit unterschiedliche Regelungen, was nicht dem Ziel der Richtlinie entsprach.²⁵⁶ Mit dem Inkrafttreten der DSGVO

²⁵¹ Vgl. Datenschutzbehörde Österreich (06.01.2021). Datenschutzrecht in Österreich

²⁵² Vgl. Datenschutzbehörde Österreich (06.01.2021). Datenschutzrecht in Österreich

²⁵³ Vgl. Sharma (2019), S. 20

²⁵⁴ Vgl. Sharma (2019), S. 20

²⁵⁵ Vgl. Sharma (2019), S. 20

²⁵⁶ Vgl. Morasch (2018), S. 21ff

wurden die unterschiedlichen Datenschutzrichtlinien in den Mitgliedstaaten vereinheitlicht und europaweit homogene Datenschutzstandards etabliert.²⁵⁷

Die DSGVO gilt für alle Unternehmen, wenn diese

- in der EU ansässig sind und personenbezogene Daten verarbeiten, unabhängig davon, wo die Datenverarbeitung stattfindet,²⁵⁸
- außerhalb der EU ansässig sind, jedoch personenbezogene Daten einer Person in der EU verarbeiten, indem sie Waren oder Dienstleistungen anbieten oder die betroffene Person beobachten.²⁵⁹

Es ist zu beachten, dass Unternehmen, die keine Niederlassung in der EU haben und personenbezogene Daten der EU-Bürger verarbeiten, einen Verantwortlichen oder Auftragsverarbeiter ernennen müssen.²⁶⁰ Ein Verantwortlicher ist in dem Sinne „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle“, die die Entscheidungen über die Verarbeitung der personenbezogenen Daten trifft.²⁶¹ Ein Auftragsverarbeiter hingegen verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen.²⁶²

6.1.1. Grundsätze für die Verarbeitung personenbezogener Daten

Die DSGVO sieht sieben Grundsätze für die rechtskonforme Verarbeitung von personenbezogenen Daten vor.

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Die Verarbeitung der personenbezogenen Daten muss unter Einhaltung der Prinzipien Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz erfolgen.²⁶³ Es bedarf also eine freiwillige Einwilligung zur Verarbeitung der persönlichen Daten der betroffenen Person. Die Rechtmäßigkeit der Verarbeitung persönlicher Daten wird im Artikel 6 ausführlicher bestimmt.

Zweckbindung

Dieser Grundsatz schreibt vor, dass die Datenerhebung nur für bereits festgelegte und rechtmäßige Zwecke erfolgen muss.²⁶⁴ Die Zweckfestlegung muss eindeutig

²⁵⁷ Vgl. Morasch (2018), S. 21ff

²⁵⁸ Vgl. Art 3 Abs 1 Datenschutzgrundverordnung (DSGVO)

²⁵⁹ Vgl. Art 3 Abs 2 Datenschutzgrundverordnung (DSGVO)

²⁶⁰ Vgl. Art 3 Abs 2 Datenschutzgrundverordnung (DSGVO)

²⁶¹ Vgl. Art 4 Nr 7 Datenschutzgrundverordnung (DSGVO)

²⁶² Vgl. Art 4 Nr 8 Datenschutzgrundverordnung (DSGVO)

²⁶³ Vgl. Art 5 Abs 1 lit a Datenschutzgrundverordnung (DSGVO)

²⁶⁴ Vgl. Art 5 Abs 1 lit b Datenschutzgrundverordnung (DSGVO)

beschrieben sein, das heißt, eine Beschreibung wie „Marketingzwecke“ ist nicht ausreichend.²⁶⁵

Datenminimierung

Die personenbezogenen Daten müssen dem Zweck angemessen und erheblich sowie auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sein.²⁶⁶

Richtigkeit

Es muss auf die sachliche Richtigkeit und Aktualität der personenbezogenen Daten geachtet werden.²⁶⁷ Die Daten, die diese Anforderungen nicht erfüllen, müssen unverzüglich gelöscht oder berichtigt bzw. aktualisiert werden.²⁶⁸

Speicherbegrenzung

Die Daten dürfen nur solange gespeichert werden, wie es für die angegebenen Zwecke, für die sie verarbeitet werden, erforderlich sind.²⁶⁹ Es bedarf einer sicheren Löschung der Daten, die nicht mehr benötigt werden.

Integrität und Vertraulichkeit

Die Verarbeitung der Daten muss in einer Weise erfolgen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.²⁷⁰

Rechenschaftspflicht

Der Verantwortliche ist für die Einhaltung der oben genannten Prinzipien verantwortlich und muss dessen Einhaltung nachweisen können.²⁷¹

6.1.2. Rechtmäßigkeit der Verarbeitung

Unter Artikel 6 der DSGVO wird die Rechtmäßigkeit der Verarbeitung bestimmt. Diese Bedingungen sind:

- Die Einwilligung zur Verarbeitung der persönlichen Daten für einen oder mehrere bestimmte Zwecke der betroffenen Person muss gegeben sein.²⁷²

²⁶⁵ Vgl. Art 5 Abs 1 lit b Datenschutzgrundverordnung (DSGVO)

²⁶⁶ Vgl. Art 5 Abs 1 lit c Datenschutzgrundverordnung (DSGVO)

²⁶⁷ Vgl. Art 5 Abs 1 lit d Datenschutzgrundverordnung (DSGVO)

²⁶⁸ Vgl. Art 5 Abs 1 lit d Datenschutzgrundverordnung (DSGVO)

²⁶⁹ Vgl. Art 5 Abs 1 lit e Datenschutzgrundverordnung (DSGVO)

²⁷⁰ Vgl. Art 5 Abs 1 lit f Datenschutzgrundverordnung (DSGVO)

²⁷¹ Vgl. Art 5 Abs 2 Datenschutzgrundverordnung (DSGVO)

²⁷² Vgl. Art 6 Abs 1 lit a Datenschutzgrundverordnung (DSGVO)

- Die Verarbeitung der personenbezogenen Daten ist erforderlich, um einen Vertrag mit der betroffenen Person oder die vorvertraglichen Maßnahmen durchzuführen.²⁷³
- Die Verarbeitung der personenbezogenen Daten ist erforderlich, um eine rechtliche Verpflichtung, der der Verantwortliche unterliegt, zu erfüllen.²⁷⁴
- Die Datenverarbeitung ist zum Schutz der lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich.²⁷⁵
- Die Verarbeitung ist erforderlich, um eine Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, wahrzunehmen.²⁷⁶
- Die Datenverarbeitung ist erforderlich, um die berechtigten Interessen des Verantwortlichen oder eines Dritten zu bewahren, sofern nicht die Interessen oder Grundrecht und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.²⁷⁷

6.1.3. Bedingungen für die Einwilligung

Jede Erfassung, Verarbeitung und Weitergabe von personenbezogenen Daten dürfen nicht ohne Einwilligung der betroffenen Person erfolgen. Die Bedingungen für die Einwilligung sind auch sehr entscheidend für die Effizienz von Big Data Anwendungen. Diese Bedingungen werden in der DSGVO unter Artikel 7 bestimmt.

- Die erste Bedingung sieht vor, dass der Verantwortliche nachweisen können muss, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.²⁷⁸
- Falls die Einwilligung der betroffenen Person in schriftlicher Form erfolgt, muss die schriftliche Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und Sprache und von anderen Sachverhalten klar unterscheidbar sein.²⁷⁹ Stellt die Einwilligungserklärung einen Verstoß gegen diese Verordnung dar, ist sie nicht verbindlich.²⁸⁰

²⁷³ Vgl. Art 6 Abs 1 lit b Datenschutzgrundverordnung (DSGVO)

²⁷⁴ Vgl. Art 6 Abs 1 lit c Datenschutzgrundverordnung (DSGVO)

²⁷⁵ Vgl. Art 6 Abs 1 lit d Datenschutzgrundverordnung (DSGVO)

²⁷⁶ Vgl. Art 6 Abs 1 lit e Datenschutzgrundverordnung (DSGVO)

²⁷⁷ Vgl. Art 6 Abs 1 lit f Datenschutzgrundverordnung (DSGVO)

²⁷⁸ Vgl. Art 7 Abs 1 Datenschutzgrundverordnung (DSGVO)

²⁷⁹ Vgl. Art 7 Abs 2 Datenschutzgrundverordnung (DSGVO)

²⁸⁰ Vgl. Art 7 Abs 2 Datenschutzgrundverordnung (DSGVO)

- Das Widerrufsrecht der Einwilligung für die betroffene Person besteht jederzeit.²⁸¹ Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.²⁸²
- Es muss sichergestellt werden, dass die Einwilligung freiwillig erteilt wurde und dass keine Erfüllung eines Vertrags oder keine Erbringung einer Dienstleistung, von der dieser Einwilligung abhängig gemacht wird.²⁸³

6.1.4. Verarbeitung besonderer Kategorien personenbezogener Daten

Unter dem Begriff personenbezogene Daten fallen alle Daten, „...die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen;...“.²⁸⁴ Die Daten, die zu einer Identifizierung von einer Person führen, sind Namen, Kennnummer, Standortdaten, besondere Merkmale, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person.²⁸⁵ Die Verarbeitung wird gemäß Artikel 4 Absatz 2 der DSGVO als einen Vorgang beschrieben, der mit oder ohne Hilfe automatisierter Verfahren im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder Bereitstellung, den Abgleich, die Einschränkung oder das Löschen ist.²⁸⁶

Weiteres fallen gemäß Artikel 9 unter personenbezogene Daten auch diese, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit, sowohl genetische und biometrische Daten als auch Gesundheitsdaten oder Daten zur sexuellen Orientierung einer natürlichen Person hervorgehen.²⁸⁷ Diese Verordnung ist jedoch nicht gültig, wenn diese Daten von der betroffenen Person veröffentlicht wurden.²⁸⁸

Unter dem Begriff „biometrische Daten“ fallen nur Lichtbilder, die mit speziellen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen.²⁸⁹ Derartige Daten fallen unter der Kategorie „sensibler Daten“ und sind nicht zu verarbeiten, es sei denn, die Verarbeitung ist

²⁸¹ Vgl. Art 7 Abs 3 Datenschutzgrundverordnung (DSGVO)

²⁸² Vgl. Art 7 Abs 3 Datenschutzgrundverordnung (DSGVO)

²⁸³ Vgl. Art 7 Abs 4 Datenschutzgrundverordnung (DSGVO)

²⁸⁴ Vgl. Art 4 Abs 1 Datenschutzgrundverordnung (DSGVO)

²⁸⁵ Vgl. Art 4 Abs 1 Datenschutzgrundverordnung (DSGVO)

²⁸⁶ Vgl. Art 4 Abs 2 Datenschutzgrundverordnung (DSGVO)

²⁸⁷ Vgl. Art 9 Abs 1 Datenschutzgrundverordnung (DSGVO)

²⁸⁸ Vgl. Art 9 Abs 2 lit e Datenschutzgrundverordnung (DSGVO)

²⁸⁹ Vgl. ErwG 51 Datenschutzgrundverordnung (DSGVO)

nach in der DSGVO oder im nationalen Recht geregelten Bestimmungen zulässig.²⁹⁰

In einzelnen Ausnahmefällen ist die Verarbeitung besonderer Kategorien von personenbezogenen Daten erlaubt. Diese Ausnahmen werden auf dem Gebiet des Arbeitsrechts und des Rechts der sozialen Sicherheit einschließlich Renten und zwecks Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen, Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren vorgesehen.²⁹¹ Die Gewährleistung der öffentlichen Gesundheit und der Verwaltung von Leistungen der Gesundheitsversorgung umfasst auch diese Ausnahmen.²⁹² Trotz dieser Ausnahmen hat die Verarbeitung der Daten besonderen Schutz der Freiheiten und Rechte der betroffenen Person zu unterliegen.²⁹³

6.1.5. Informationspflicht

Bei einer Verarbeitung von personenbezogenen Daten muss der Verantwortliche die Informationspflichten der DSGVO beachten. Hier muss die betroffene Person zum Zeitpunkt der Datenerhebung über die folgenden Punkte aufgeklärt werden:

- Name und Kontaktdaten des Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten,^{294 295}
- Zwecke der Verarbeitung personenbezogener Daten und Rechtsgrundlage für die Verarbeitung,²⁹⁶
- Kategorien der Empfänger der Daten,²⁹⁷
- Information über Übermittlung der Daten an ein Drittland oder eine internationale Organisation,²⁹⁸
- die Speicherdauer dieser Daten oder falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer,²⁹⁹
- Rechte des Betroffenen auf Auskunft über die betreffenden Daten, auf Berichtigung oder Löschung, auf Einschränkung der Verarbeitung,

²⁹⁰ Vgl. ErwG 51 Datenschutzgrundverordnung (DSGVO)

²⁹¹ Vgl. ErwG 51 Datenschutzgrundverordnung (DSGVO)

²⁹² Vgl. ErwG 51 Datenschutzgrundverordnung (DSGVO)

²⁹³ Vgl. ErwG 54 Datenschutzgrundverordnung (DSGVO)

²⁹⁴ Vgl. Art 13 Abs 1 lit a Datenschutzgrundverordnung (DSGVO)

²⁹⁵ Vgl. Art 13 Abs 1 lit b Datenschutzgrundverordnung (DSGVO)

²⁹⁶ Vgl. Art 13 Abs 1 lit c Datenschutzgrundverordnung (DSGVO)

²⁹⁷ Vgl. Art 13 Abs 1 lit e Datenschutzgrundverordnung (DSGVO)

²⁹⁸ Vgl. Art 13 Abs 1 lit f Datenschutzgrundverordnung (DSGVO)

²⁹⁹ Vgl. Art 13 Abs 2 lit a Datenschutzgrundverordnung (DSGVO)

Widerspruchsrecht gegen die Verarbeitung und Recht auf Datenübertragbarkeit,^{300 301}

- Recht auf Beschwerde bei einer Aufsichtsbehörde,³⁰²
- Folgen bei Nichtbereitstellung der personenbezogenen Daten und ob es gesetzlich oder vertraglich vorgeschrieben erforderlich ist, diese Daten bereitzustellen und³⁰³
- Bestehen und Auswirkung einer automatisierten Entscheidungsfindung einschließlich Profiling.³⁰⁴

Bei Erhebung dieser Daten bei einem Dritten ist zusätzlich noch die Quelle, aus der diese Daten stammen und gegebenenfalls, ob sie aus einer öffentlichen Quelle stammen, anzugeben.³⁰⁵

6.1.6. Profiling

Der Begriff Profiling bedeutet „...jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.“³⁰⁶

Big Data Anwendungen verwenden Profiling, um die große Menge an Daten für aussagekräftige Datenanalysen vorzubereiten. Auch Cambridge Analytica nutzte diesen Prozess, um Werbebotschaften an gezielten Personen aufgrund derer gesammelten personenbezogenen Daten zu versenden. Profiling stellt sozusagen einen wichtigen Teil der Big Data Analysen dar. Die DSGVO untersagt das Profiling nicht, jedoch ist dieses Verfahren an allen Regelungen der DSGVO verbunden, die jegliche Verarbeitung von personenbezogenen Daten regeln.³⁰⁷

Eine weitere Regelung besagt, dass die betroffene Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling

³⁰⁰ Vgl. Art 13 Abs 2 lit b Datenschutzgrundverordnung (DSGVO)

³⁰¹ Vgl. Art 13 Abs 2 lit c Datenschutzgrundverordnung (DSGVO)

³⁰² Vgl. Art 13 Abs 2 lit d Datenschutzgrundverordnung (DSGVO)

³⁰³ Vgl. Art 13 Abs 2 lit e Datenschutzgrundverordnung (DSGVO)

³⁰⁴ Vgl. Art 13 Abs 2 lit f Datenschutzgrundverordnung (DSGVO)

³⁰⁵ Vgl. Art 14 Abs 2 lit f Datenschutzgrundverordnung (DSGVO)

³⁰⁶ Vgl. Art 4 Abs 4 Datenschutzgrundverordnung (DSGVO)

³⁰⁷ Vgl. ErwG 71 Datenschutzgrundverordnung (DSGVO)

– beruhenden Entscheidung unterworfen zu werden, wodurch rechtliche oder andere ernste Folgen für diese Person entstehen könnten.³⁰⁸

6.1.7. Technische Maßnahmen zur sicheren Datenverarbeitung

Unternehmen, die Big Data Technologien anwenden, müssen bestimmte technische und organisatorische Maßnahmen treffen, um die Sicherheit der Datenverarbeitung und den Schutz der betroffenen Person zu gewährleisten und die unter Artikel 5 Absatz 1 geregelten Datenschutzgrundsätze einzuhalten. Die DSGVO schreibt vor, dass der Verantwortliche unter Berücksichtigung des Stands der Technik und der Art bzw. Zwecke der Verarbeitung und damit verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen treffen muss.³⁰⁹ Als geeignete Maßnahmen werden in der DSGVO unter Artikel 32 Absatz 1 Folgendes angegeben:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten, oder³¹⁰
- die dauerhafte Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung, oder³¹¹
- eine rasche Wiederherstellung der Fähigkeit, Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall, oder³¹²
- ein Verfahren, das die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ermöglicht.³¹³

Unter Pseudonymisierung gemäß Artikel 4 Absatz 5 der DSGVO wird verstanden, dass die Verarbeitung personenbezogener Daten in einer Art und Weise erfolgt, sodass diese Daten nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, wobei es auch berücksichtigt werden muss, dass die zusätzlichen Informationen, mit denen es eine Identifizierung der Person möglich ist, gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen

³⁰⁸ Vgl. Art 22 Abs 1 Datenschutzgrundverordnung (DSGVO)

³⁰⁹ Vgl. Art 25 Abs 1 Datenschutzgrundverordnung (DSGVO)

³¹⁰ Vgl. Art 32 Abs 1 lit a Datenschutzgrundverordnung (DSGVO)

³¹¹ Vgl. Art 32 Abs 1 lit b Datenschutzgrundverordnung (DSGVO)

³¹² Vgl. Art 32 Abs 1 lit c Datenschutzgrundverordnung (DSGVO)

³¹³ Vgl. Art 32 Abs 1 lit d Datenschutzgrundverordnung (DSGVO)

unterliegen müssen.³¹⁴ Durch Pseudonymisierung der personenbezogenen Daten können die Risiken für die betroffene Personen sinken.³¹⁵

Eine Anonymisierung der personenbezogenen Daten führt dazu, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.³¹⁶ In diesem Fall ist es zu beachten, dass die Grundsätze des Datenschutzes nicht für die anonymisierten Informationen gelten.³¹⁷

Der Unterschied zwischen Pseudonymisierung und Anonymisierung liegt darin, dass die pseudonymisierten Daten später wieder identifiziert bzw. den Personen zugeordnet werden können, wobei dies bei anonymisierten Daten nicht möglich ist, da die personenbezogenen Daten nach der Anonymisierung vernichtet werden.³¹⁸

Es ist jedoch festzuhalten, dass anonymisierte Daten nicht für alle Big Data Analysen ausreichend sind, wie zum Beispiel Direktmarketing, denn je stärker die Anonymisierung ist, desto geringer ist der Informationsgehalt der Daten.³¹⁹ Der geringe Informationsgehalt der Daten bringt einen geringen Nutzen für Big Data Analysen.³²⁰

6.1.8. Datenschutz-Folgenabschätzung

Die Nutzung von Big Data Technologien bringen aufgrund der verarbeiteten Daten viele datenschutzrechtliche Risiken mit sich. Unternehmen, die Daten verarbeiten, müssen eine Datenschutz-Folgenabschätzung durchführen, wenn die „...*Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zu Folge...*“ hat, so muss der Verantwortliche vorab eine Abschätzung der Folgen des Verarbeitungsprozesses für den Schutz der personenbezogenen Daten durchführen.³²¹

Eine Datenschutz-Folgenabschätzung ist dann zwingend notwendig, wenn:

- eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die aufgrund automatisierter Verarbeitung – einschließlich Profiling – stattfindet und als eine Grundlage für Entscheidungen dient, die rechtliche oder andere ähnliche Folgen für die betroffene Person mit sich bringen,³²²

³¹⁴ Vgl. Art 4 Abs 5 Datenschutzgrundverordnung (DSGVO)

³¹⁵ Vgl. ErwG 28 Datenschutzgrundverordnung (DSGVO)

³¹⁶ Vgl. ErwG 26 Datenschutzgrundverordnung (DSGVO)

³¹⁷ Vgl. ErwG 26 Datenschutzgrundverordnung (DSGVO)

³¹⁸ Vgl. BMVIT (2017), S. 33

³¹⁹ Vgl. BMVIT (2017), S. 107

³²⁰ Vgl. BMVIT (2017), S. 107

³²¹ Vgl. Art 35 Abs 1 Datenschutzgrundverordnung (DSGVO)

³²² Vgl. Art 35 Abs 2 lit a Datenschutzgrundverordnung (DSGVO)

- eine umfangreiche Verarbeitung der Daten erfolgt, die unter besonderen Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder unter personenbezogenen Daten über strafrechtliche Verteilungen und Straftaten gemäß Artikel 10 fallen, oder³²³
- öffentlich zugängliche Bereiche systematisch und umfangreich überwacht werden.³²⁴

6.2. Datenschutzgesetz in Österreich

Das österreichische Datenschutzgesetz ergänzt die DSGVO und regelt den Schutz der personenbezogenen Daten in Österreich. Das Datenschutzgesetz von 2000 wurde im Jahr 2018 durch das Datenschutz-Anpassungsgesetz 2018 und Datenschutz-Deregulierungsgesetz 2018 stark verändert.³²⁵ Die neuen Regelungen sind am 25. Mai 2018 in Kraft getreten. In Österreich regeln den Datenschutz sowohl die DSGVO als auch das Datenschutzgesetz.

6.2.1. Grundrecht auf Datenschutz

„Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.“³²⁶

Im ersten Artikel des Datenschutzgesetzes wird der Datenschutz für Menschen als Grundrecht erkannt. Die Verwendung der personenbezogenen Daten ist nur dann zulässig, wenn es nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt.³²⁷ Besondere Bestimmungen zur Verwendung der personenbezogenen Daten werden in den nächsten Kapiteln erläutert.

³²³ Vgl. Art 35 Abs 2 lit b Datenschutzgrundverordnung (DSGVO)

³²⁴ Vgl. Art 35 Abs 2 lit c Datenschutzgrundverordnung (DSGVO)

³²⁵ Vgl. Datenschutzbehörde Österreich (06.01.2021). Datenschutzrecht in Österreich

³²⁶ Vgl. Art 1 Abs 1 Datenschutzgesetz (DSG)

³²⁷ Vgl. Art 1 Abs 2 Datenschutzgesetz (DSG)

6.2.2. Datengeheimnis

Dienstnehmer eines Unternehmens müssen die personenbezogenen Daten, die ihnen ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, geheim halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht.³²⁸ Die Datenübermittlung durch einen Mitarbeiter darf nur dann erfolgen, wenn diese ausdrücklich vom Arbeitgeber angeordnet wird.³²⁹ Das Datengeheimnis muss auch nach Beendigung des Arbeitsverhältnisses zum Verantwortlichen oder Auftragsverarbeiter eingehalten werden.³³⁰ Der Verantwortliche und der Auftragsverarbeiter haben die Pflicht, die betroffenen Mitarbeiter über die Folgen einer Verletzung des Datengeheimnisses zu informieren.³³¹ Auf Grund des verfassungsrechtlichen Weisungsrecht darf die Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung keine Folgen für den betroffenen Mitarbeiter haben.³³²

6.2.3. Datenverarbeitungen zu spezifischen Zwecken

Das Datenschutzgesetz erlaubt die Datenverarbeitung unter bestimmten Voraussetzungen. Eine Voraussetzung ist unter der Zweckbestimmung erklärt. Die Verarbeitung von personenbezogenen Daten kann dann erfolgen, wenn sie für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke verarbeitet werden.³³³ Eine andere Voraussetzung ist die Art der Ermittlung dieser personenbezogenen Daten. Nur diese personenbezogenen Daten können zu diesen Zwecken verarbeitet werden, die

- öffentlich zugänglich sind,³³⁴
- der Verantwortliche für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder³³⁵
- für den Verantwortlichen pseudonymisierte personenbezogene Daten sind und er die Identität der betroffenen Personen mit rechtlich zulässigen Mitteln nicht bestimmen kann.³³⁶

³²⁸ Vgl. Art 6 Abs 1 Datenschutzgesetz (DSG)

³²⁹ Vgl. Art 6 Abs 2 Datenschutzgesetz (DSG)

³³⁰ Vgl. Art 6 Abs 2 Datenschutzgesetz (DSG)

³³¹ Vgl. Art 6 Abs 3 Datenschutzgesetz (DSG)

³³² Vgl. Art 6 Abs 4 Datenschutzgesetz (DSG)

³³³ Vgl. Art 7 Abs 1 Datenschutzgesetz (DSG)

³³⁴ Vgl. Art 7 Abs 1 Z 1 Datenschutzgesetz (DSG)

³³⁵ Vgl. Art 7 Abs 1 Z 2 Datenschutzgesetz (DSG)

³³⁶ Vgl. Art 7 Abs 1 Z 3 Datenschutzgesetz (DSG)

Falls diese Voraussetzungen und andere gesetzliche Vorschriften für die Datenverarbeitung nicht erfüllt sind, muss die Einwilligung der betroffenen Person geholt werden oder von der Datenschutzbehörde genehmigt werden.³³⁷

6.2.4. Bildverarbeitung

Artikel 12 des Datenschutzgesetzes regelt die Zulässigkeit einer Bildaufnahme. Der Begriff Bildaufnahme wird hier definiert als „*die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken.*“³³⁸ Zu einer Bildaufnahme in diesem Sinne gehören zusätzlich dabei mitverarbeitete akustische Informationen.³³⁹ Eine derartige Bildaufnahme ist unter bestimmten Vorgaben zulässig, wenn

- sie im lebenswichtigen Interesse einer Person erforderlich ist,³⁴⁰
- eine Einwilligung von der betroffenen Person erteilt wurde,³⁴¹
- sie durch eine gesetzliche Anordnung erlaubt wurde, oder³⁴²
- im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.³⁴³

Berechtigte Interessen des Verantwortlichen oder eines Dritten und die Verhältnismäßigkeit ist gegeben, wenn

- sie dem Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, oder³⁴⁴
- sie dem Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen und es aufgrund der bereits erfolgten Rechtsverletzungen oder des besonderen Gefährdungspotenzials des Ortes erforderlich ist, oder³⁴⁵

³³⁷ Vgl. Art 7 Abs 2 Datenschutzgesetz (DSG)

³³⁸ Vgl. Art 12 Abs 1 Datenschutzgesetz (DSG)

³³⁹ Vgl. Art 12 Abs 1 Datenschutzgesetz (DSG)

³⁴⁰ Vgl. Art 12 Abs 2 Z 1 Datenschutzgesetz (DSG)

³⁴¹ Vgl. Art 12 Abs 2 Z 2 Datenschutzgesetz (DSG)

³⁴² Vgl. Art 12 Abs 2 Z 3 Datenschutzgesetz (DSG)

³⁴³ Vgl. Art 12 Abs 2 Z 4 Datenschutzgesetz (DSG)

³⁴⁴ Vgl. Art 12 Abs 3 Z 1 Datenschutzgesetz (DSG)

³⁴⁵ Vgl. Art 12 Abs 3 Z 2 Datenschutzgesetz (DSG)

- es auf ein privates Dokumentationsinteresse erfolgt, das nicht auf die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung einer Person eignen, gerichtet ist.³⁴⁶

Eine Bildverarbeitung ist dann untersagt, wenn

- die Bildaufnahme ohne eine Einwilligung der betroffenen Person,³⁴⁷
- diese zum Zweck der Kontrolle von Arbeitnehmern erfolgt,³⁴⁸
- zum automationsunterstützten Abgleich von mittels Bildaufnahmen gewonnen personenbezogenen Daten ohne ausdrückliche Einwilligung und für das Erstellen von Persönlichkeitsprofilen mit anderen personenbezogenen Daten genutzt wird, oder³⁴⁹
- die personenbezogenen Daten anhand von besonderen Kategorien personenbezogener Daten gemäß Artikel 9 der DSGVO, die aus Bildaufnahmen ermittelt wurden, zur Auswertung genutzt werden.³⁵⁰

Der Verantwortliche ist dazu verpflichtet, geeignete Datensicherheitsmaßnahmen zu ergreifen und den Zugang zu einer Bildaufnahme und eine nachträgliche Veränderung derselben durch Unbefugte auszuschließen.³⁵¹ Die Verarbeitungsvorgänge sind, außer in Fällen einer Echtzeitüberwachung, zu protokollieren und alle aufgenommenen personenbezogenen Daten sind vom Verantwortlichen zu löschen, wenn sie nicht mehr benötigt werden und wenn keine gesetzlich vorgesehene Aufbewahrungspflicht besteht.^{352 353} Es besteht eine Kennzeichnungspflicht der Bildaufnahme für den Verantwortlichen.³⁵⁴ Die Auskunft der Identität des Verantwortlichen einer Bildaufnahme unterliegt der Auskunftspflicht gemäß Artikel 15 der DSGVO und kann von jeder betroffenen Person begehrt werden.³⁵⁵

³⁴⁶ Vgl. Art 12 Abs 3 Z 3 Datenschutzgesetz (DSG)

³⁴⁷ Vgl. Art 12 Abs 4 Z 1 Datenschutzgesetz (DSG)

³⁴⁸ Vgl. Art 12 Abs 4 Z 2 Datenschutzgesetz (DSG)

³⁴⁹ Vgl. Art 12 Abs 4 Z 3 Datenschutzgesetz (DSG)

³⁵⁰ Vgl. Art 12 Abs 4 Z 4 Datenschutzgesetz (DSG)

³⁵¹ Vgl. Art 13 Abs 1 Datenschutzgesetz (DSG)

³⁵² Vgl. Art 13 Abs 2 Datenschutzgesetz (DSG)

³⁵³ Vgl. Art 13 Abs 3 Datenschutzgesetz (DSG)

³⁵⁴ Vgl. Art 13 Abs 6 Datenschutzgesetz (DSG)

³⁵⁵ Vgl. Art 13 Abs 7 Datenschutzgesetz (DSG)

6.2.5. Verarbeitung personenbezogener Daten für Zwecke der Sicherheitspolizei

Die Verarbeitung der personenbezogenen Daten durch die Sicherheitspolizei hat im DSG eine bestimmte Regelung. Diese Bestimmungen gelten „...für die Verarbeitung personenbezogener Daten durch zuständige Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum Zweck der nationalen Sicherheit, des Nachrichtendienstes und der militärischen Eigensicherung.“³⁵⁶ Die personenbezogenen Daten sind hier nach Kategorien betroffener Personen zu unterscheiden, die aufgrund bestimmter Tatsachen konkret verdächtig sind, eine strafbare Handlung begangen zu haben, oder gegen die aufgrund bestimmter Tatsachen ein begründeter Verdacht besteht, dass sie in naher Zukunft eine strafbare Handlung begehen werden, oder verurteilte Straftäter, oder Opfer einer Straftat und sonstige Personen, die im Zusammenhang mit einer Straftat stehen.³⁵⁷ Die Verarbeitung kann auch für andere Zwecke und Übermittlung erfolgen, wenn diese durch denselben Verantwortlichen und in dem Anwendungsbereich gemäß Artikel 36 Absatz 1 des DSGs liegen, ansonsten muss eine gesetzliche Regelung für die Zulässigkeit bestehen.³⁵⁸ Das DSG sieht auch eine Einschränkung der Informationspflicht vor, wenn diese einem Gesetz unterliegen oder zu bestimmten Zwecken dienen.³⁵⁹ Eine Einschränkung der Informationspflicht ist in den folgenden Fällen möglich:

- Gewährleistung, dass die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung nicht beeinträchtigt werden,³⁶⁰
- zum Schutz der öffentlichen Sicherheit,³⁶¹
- zum Schutz der nationalen Sicherheit,³⁶²
- zum Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich,³⁶³
- zum Schutz der militärischen Eigensicherung oder³⁶⁴
- zum Schutz der Rechte und Freiheiten anderer.³⁶⁵

³⁵⁶ Vgl. Art 36 Abs 1 Datenschutzgesetz (DSG)

³⁵⁷ Vgl. Art 37 Abs 4 Datenschutzgesetz (DSG)

³⁵⁸ Vgl. Art 40 Datenschutzgesetz (DSG)

³⁵⁹ Vgl. Art 43 Abs 4 Datenschutzgesetz (DSG)

³⁶⁰ Vgl. Art 43 Abs 4 Z 1 Datenschutzgesetz (DSG)

³⁶¹ Vgl. Art 43 Abs 4 Z 2 Datenschutzgesetz (DSG)

³⁶² Vgl. Art 43 Abs 4 Z 3 Datenschutzgesetz (DSG)

³⁶³ Vgl. Art 43 Abs 4 Z 4 Datenschutzgesetz (DSG)

³⁶⁴ Vgl. Art 43 Abs 4 Z 5 Datenschutzgesetz (DSG)

³⁶⁵ Vgl. Art 43 Abs 4 Z 6 Datenschutzgesetz (DSG)

7. Conclusio

Big Data bietet großes Potenzial für wichtige Innovationen, wirtschaftliche Wertschöpfung, gesellschaftlichen Fortschritt und das Gesundheitswesen. Mit Predictive Analytics können die besten Behandlungsmethoden für einen Patienten basierend auf die medizinische Vorgeschichte bestimmt und angewendet werden. Mit Big Data Lösungen sind Unternehmen in der Lage, aufgrund der präzisen Prognosen, die mit Big Data Auswertungen erlangt werden, zukunftsichere Entscheidungen zu treffen. Doch die große Menge an Daten hat auch ein enormes Potenzial, Schaden anzurichten und Grundrechte, wie Datenschutz, zu verletzen. Deshalb müssen Unternehmen und Regierungen Maßnahmen setzen, um den Datenmissbrauch zu minimieren bzw. zu verhindern.

Die gesetzlichen Lockerungen für die Überwachung der Gesellschaft verlangt besondere Aufmerksamkeit, denn diese Einschränkungen können mit der Zeit zu einem Überwachungsstaat führen. Die Gesetze, die nach einem Terroranschlag bzw. jeder Bedrohung der nationalen Sicherheit eingeführt werden, schränken den Datenschutz ein.³⁶⁶ Datenschutz ist ein Grundrecht und gewährleistet die Selbstbestimmung über die Verarbeitung der eigenen personenbezogenen Daten und benötigt strengere Regelungen.

Big Data Technologien und Analysen sollten unter demokratischer Überwachung vom Parlament stehen und nicht nur von einer Person der Regierung oder Geheimdienst kontrolliert werden können.³⁶⁷

Der Einsatz solcher Big Data Technologien sollte auf demokratischen und wissenschaftlichen Prinzipien beruhen und durch Teams führender Wissenschaftler, wie Psychologen, Soziologen, Juristen und Informatiker erfolgen.³⁶⁸

Die Technologieunternehmen, die enorme Menge an Daten sammeln und mit diesen handeln, sollen streng kontrolliert und bei Verstößen gegen die DSGVO bzw. das DSG bestraft werden, sodass es wirksam und abschreckend ist.

Es empfiehlt sich, jede Aktivität bei Nutzung dieser Technologien aufzuzeichnen und auf Anfrage der Bürger diese Protokolle zu veröffentlichen.³⁶⁹ Jeder Bürger soll das Recht haben, sich über die staatliche Nutzung deren personenbezogenen Daten zu informieren.

Ein weiteres Problem stellt das Fehlen der exakt definierten rechtlichen Anforderungen an die Stärke der Anonymisierung von personenbezogenen Daten dar.³⁷⁰ Es

³⁶⁶ Vgl. BMVIT (2017), S. 17

³⁶⁷ Vgl. Helbing (2019), S. 29

³⁶⁸ Vgl. Helbing (2019), S. 29ff

³⁶⁹ Vgl. Helbing (2019), S. 30

³⁷⁰ Vgl. BMVIT (2017), S. 107ff

müssen auch Maßnahmen gesetzt werden, um das Umgehen der Anonymisierung durch fortgeschrittene technologische Entwicklungen zu verhindern.³⁷¹

Abschließend lässt sich festhalten, dass die Demokratie ein „digitales Upgrade“ benötigt, um mit dem rapiden digitalen Wandel der Welt mithalten zu können.³⁷² Die Überwachung durch Unternehmen und Staaten bedarf besonderer Aufmerksamkeit, denn es stellt nicht nur ein Problem für die individuelle Meinungsbildung und Selbstbestimmung der Menschen dar, sondern auch für die Demokratie, deren Grundsätze durch die immer stärker werdende Überwachung und Manipulation der politischen Meinungsbildung der Bevölkerung verletzt werden.

³⁷¹ Vgl. BMVIT (2017), S. 108

³⁷² Vgl. Helbing (2017), S. 30

8. Anhang

A

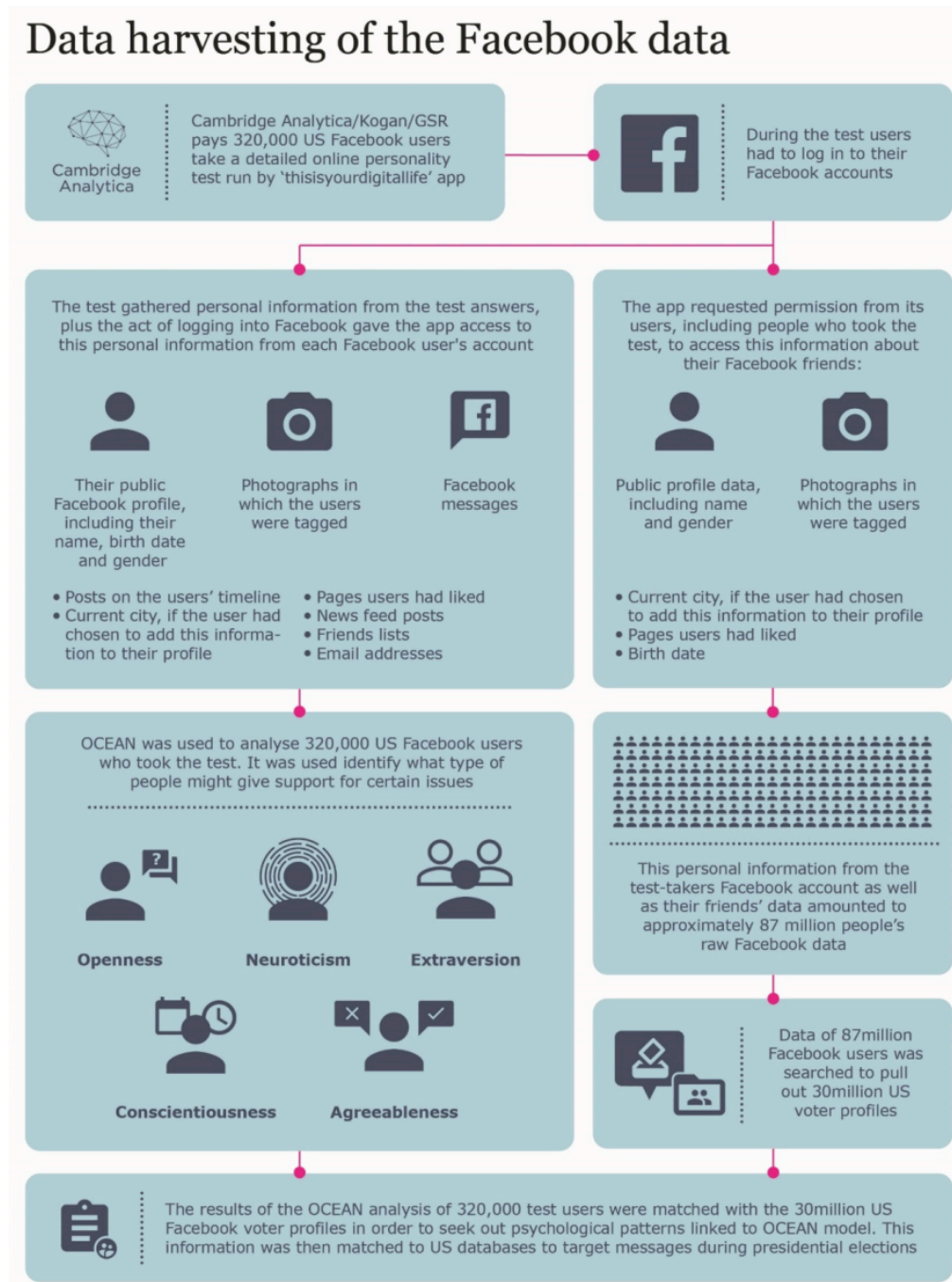


Abbildung 4: Erfassung der Facebook-Daten³⁷³

³⁷³ Vgl. ICO (2018), S. 17

9. Literaturverzeichnis

- Bigo, D. et al., 2013. *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, s.l.: CEPS Paper.
- Black Mirror*, "Nosedive", Staffel 3, Folge 1. 2016. [Film] Regie: Charlie Brooker. s.l.: Netflix.
- BMVIT, 2017. *Big Data, Innovation und Datenschutz*, Wien: SBA Research, Wirtschaftsuniversität Wien.
- Chandel, S. et al., 2019. *The Golden Shield Project of China: A Decade Later – An in-depth study of the Great Firewall*, Nanjing, China: New York Institute of Technology.
- Chen, Y. & Cheung, A. S., 2017. *The Transparent Self under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System*, s.l.: Social Science Research Network.
- Chungheng, L., 2019. *Multiple Social Credit Systems in China*, s.l.: Economic Sociology: The European Electronic Newsletter, 2019, 21 (1).
- Cisco, 2020. Cisco Annual Internet Report (2018–2023), s.l.: Cisco.
- Creemers, R., 2018. *China's Social Credit System: An Evolving Practice of Control*, s.l.: Leiden University - Leiden Institute for Area Studies.
- Datta, A., Tschantz, M. C. & Datta, A., 2015. *Automated Experiments on Ad Privacy Settings*, s.l.: Cornell University.
- Denham, E., 2020. *ICO investigation into use of personal information and political influence.*, s.l.: ICO.
- Farkisch, K., 2011. *Data-Warehouse-Systeme kompakt: Aufbau, Architektur, Grundfunktionen*. s.l.:Springer.
- Farnan, O., Darer, A. & Wright, J., 2016. *Poisoning the Well – Exploring the Great Firewall's Poisoned DNS Responses*, Oxford, UK: University of Oxford.
- Fuchs, C., 2010. Facebook, Web 2.0 und ökonomische Überwachung. In: *Datenschutz und Datensicherheit - DuD*. s.l.:Springer, pp. 453-458.
- Gartner, R., 2016. *Metadata: Shaping Knowledge from Antiquity to the Semantic Web*. s.l.:Springer.
- Helbing, D., 2019. *Towards Digital Enlightenment*. s.l.:Springer.
- HIS Markit, 2020. *Video Surveillance Installed Base Report – 2019*, s.l.: HIS Markit.
- Holmes, D. E., 2017. *Big Data: A Very Short Introduction*. s.l.:Oxford University Press.
- ICO, 2018. *Democracy Disrupted? Personal Information and Political Influence*, s.l.: ICO.
- ICO, 2018. *Investigation into the use of data analytics in political campaigns - Investigation Update*, s.l.: ICO.

- Kaiser, B., 2019. *Targeted: My Inside Story of Cambridge Analytica and How Trump, Brexit and Facebook broke Democracy*. s.l.:Harper Collins Publishers.
- Kerr, J., 2019. *The Russian Model of Digital Control and Its Significance*, Artificial Intelligence, China, Russia, and the Global Order: Air University Press.
- Liang, F., Das, V., Kostyuk, N. & Hussain, M. M., 2018. *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, Special Issue: Social Media and Big Data in China: Vol. 10 Issue 4: Policy Studies Organization.
- Loideain, N., 2015. *EU Law and Mass Internet Metadata Surveillance in the Post Snowden Era*. University of Cambridge: s.n.
- Lothar, L., 2008. *Persönlichkeitspsychologie*. s.l.:Kohlhammer.
- Maréchal, N., 2016. *Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy*, s.l.: University of Southern California.
- Meissner, M. & Wübbeke, J., 2016. *IT-backed authoritarianism: Information technology enhances central authority and control capacity under Xi Jinping*, s.l.: Merics.
- Morasch, O., 2018. *Datenverarbeitung im Beschäftigungskontext*. s.l.:Nomos.
- Morgus, R., 2019. *The Spread of Russian Digital Authoritarianism*, Artificial Intelligence, China, Russia, and the Global Order: Air University Press.
- Raghupathi, W. & Raghupathi V., 2014. *Big Data Analytics in healthcare: promise and potential*, s.l.: Health Information Science and Systems
- Raj, P., Poongodi, T., Khari, M. & Balusamy, B., 2020. *The Internet of Things and Big Data Analytics*. s.l.:CRC Press.
- Reinsel, G. R., 2017. *Data Age 2025: The Evolution of Data to Life-Critical*, IDC: s.n.
- Schön, D., 2016. *Planung und Reporting: Grundlagen, Business Intelligence, Mobile BI und Big Data-Analytics*. s.l.:Springer.
- Schaar, P., 2015. *Globale Überwachung und digitale Souveränität*, Z Außen Sicherheitspolit 8:447–459: Springer.
- Schaefer, K. & Yin, E., 2019. *Understanding China's Social Credit System*, s.l.: Trivium China.
- SCMPR, 2020. *China Internet Report 2020*, s.l.: South China Morning Post Research.
- Sharma, S., 2019. *Data Privacy and GDPR Handbook*. s.l.:Shiley.
- Sweeney, L., 2013. *Discrimination in Online Ad Delivery*, s.l.: Harvard University.
- Weber, V., 2017. *Why China's internet censorship model will prevail over Russia's Authors*, s.l.: Council on Foreign Relations.
- Xiao, Q., 2019. *The Road to Digital Unfreedom: President Xi's Surveillance State.*, s.l.: Journal of Democracy 30, no. 1.

Internetquellen

- Anti, M., 2012. *Behind the Great Firewall of China*. Verfügbar unter: https://www.ted.com/talks/michael_anti_behind_the_great_firewall_of_china, Zugriff am 16.11.2020.
- Barme, G. R. & Ye, S., 1997. *Wired - The Great Firewall of China*. Verfügbar unter: <https://www.wired.com/1997/06/china-3/>, Zugriff am 12.11.2020.
- Baumgärtner, M., Gude, H., Rosenbach, M. & Schindler, J., 2015. *Spiegel - Neue Spionageaffäre erschüttert BND*. Verfügbar unter: <https://www.spiegel.de/politik/deutschland/ueberwachung-neue-spionageaffaere-erschuettert-bnd-a-1030191.html>, Zugriff am 11.12.2020.
- BBC, 2017. *Social media and censorship in China: how is it different to the West?*. Verfügbar unter: <https://www.bbc.com/news/newsbeat-41398423>, Zugriff am 11.11. 2020.
- Biermann, K., 2015. *Zeit Online - BND liefert NSA 1,3 Milliarden Metadaten – jeden Monat*. Verfügbar unter: <https://www.zeit.de/politik/deutschland/2015-05/bnd-nsa-milliarden-metadaten/komplettansicht>, Zugriff am 11.12.2020.
- Chew, C. W., 2018. *Medium - How It Works: Great Firewall of China*. Verfügbar unter: <https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475>, Zugriff am 12.11.2020.
- Creemers, R., Triolo, P. & Webster, G., 2018. *Cyber Security Law 2016*. Verfügbar unter: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>, Zugriff am 25.11.2020.
- Datenschutzbehörde Österreich, kein Datum *Datenschutzrecht in Österreich*. Verfügbar unter: <https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html>, Zugriff am 06.01.2021.
- Davidson, H., 2020. *The Guardian - Chinese city plans to turn coronavirus app into permanent health tracker*. Verfügbar unter: <https://www.theguardian.com/world/2020/may/26/chinese-city-plans-to-turn-coronavirus-app-into-permanent-health-tracker>, Zugriff am 17.11.2020.
- Denyer, S., 2018. *The Washington Post - Beijing bets on facial recognition in a big drive for total surveillance*. Verfügbar unter: <https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/>, Zugriff am 25.11.2020.
- Deuber, L., 2017. *Wirtschaftswoche - Warum China zum Entwicklungsland wird*. Verfügbar unter: <https://www.wiwo.de/politik/ausland/zunehmende-beschaerungen-im-netz-china-hat-den-groessten-digitalen-markt-der-welt/20661594-2.html>, Zugriff am 16.11.2020.
- Domo, 2020. *Data never sleeps 8.0*. Verfügbar unter: <https://www.domo.com/learn/data-never-sleeps-8>, Zugriff am 20.12.2020.

Facebook, 2021. *Our Response to the Violence in Washington*. Verfügbar unter: <https://about.fb.com/news/2021/01/responding-to-the-violence-in-washington-dc/>, Zugriff am 31.01.2021.

Freedom House, 2020. *The Pandemic's Digital Shadow*. Verfügbar unter: <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow>. Zugriff am 06.11.2020.

FTC, 2019. *FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*. Verfügbar unter: <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>, Zugriff am 05.01.2021.

Gan, N. & Culver, D., 2020. *CNN - China is fighting the coronavirus with a digital QR code. Here's how it works*. Verfügbar unter: <https://edition.cnn.com/2020/04/15/asia/china-coronavirus-qr-code-intl-hnk/index.html>, Zugriff am 17.11.2020.

Gartner, *Glossar - Big Data*. Verfügbar unter: <https://www.gartner.com/en/information-technology/glossary/big-data>, Zugriff am 22.12.2020.

Gartner, *Glossar - Data Broker*. Verfügbar unter: <https://www.gartner.com/en/information-technology/glossary/data-broker>, Zugriff am 02.01.2021.

Gartner, *Glossar - Descriptive Analytics*. Verfügbar unter: <https://www.gartner.com/en/information-technology/glossary/descriptive-analytics>, Zugriff am 25.12.2020.

Gartner, *Glossar - Diagnostic Analytics*. Verfügbar unter: <https://www.gartner.com/en/information-technology/glossary/diagnostic-analytics>, Zugriff am 25.12.2020.

Gartner, *Glossar - Predictive Analytics*. Verfügbar unter: <https://www.gartner.com/en/information-technology/glossary/predictive-analytics-2>, Zugriff am 25.12.2020.

Haas, B., 2017. *The Guardian - Man in China sentenced to five years' jail for running VPN*. Verfügbar unter: <https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn>, Zugriff am 13.11.2020.

Hayden, M., 2014. *The Johns Hopkins Foreign Affairs Symposium Presents: The Price of Privacy: Re-Evaluating the NSA*. (Youtube). Verfügbar unter: https://www.youtube.com/watch?v=kV2HDM86Xgl&ab_channel=JohnsHopkinsUniversity, Zugriff am 25.12.2020

HazelCast, *Glossar - CAP Theorem*. Verfügbar unter: <https://www.hazelcast.com/glossary/cap-theorem>, Zugriff am 27.12.2020.

Hoppenstadt, M. & Wiedmann-Schmidt, W., 2020. *Spiegel - So überwacht der BND das Internet*. Verfügbar unter: <https://www.spiegel.de/netzwelt/netzpolitik/bundesnachrichtendienst-so-ueberwacht-der-bnd-das-internet-a-216ebe9a-6f22-4883-b1c9-ac5d1442497a>, Zugriff am 11.12.2020.

IDC, 2020. *IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data*. Verfügbar unter:

<https://www.idc.com/getdoc.jsp?containerId=prUS46286020>, Zugriff am 20.12.2020.

Jiang, S., 2017. *Reuters - China cracks down on unauthorized internet connections*.

Verfügbar unter: <https://www.reuters.com/article/us-china-internet-idUSKBN15715U>, Zugriff am 13.11.2020.

Kobie, N., 2019. *Wired - The complicated truth about China's social credit system*.

Verfügbar unter: <https://www.wired.co.uk/article/china-social-credit-system-explained>, Zugriff am 30.11.2020.

Kurier, 2020. *Mehr als eine Billion Dollars Schaden durch Cyberkriminalität*. Verfügbar unter:

<https://kurier.at/wirtschaft/mehr-als-eine-billion-dollar-schaden-durch-cyberkriminalitaet/401122353>, Zugriff am 31.01.2021.

Lewis, J. A., 2014. *CSIS - Reference Note on Russian Communications Surveillance*.

Verfügbar unter: <https://www.csis.org/analysis/reference-note-russian-communications-surveillance>, Zugriff am 08.12.2020.

MacAskill, E. et al., 2013. *The Guardian - GCHQ taps fibre-optic cables for secret access to world's communications*. Verfügbar unter:

<https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa?guccounter=1&guceq=Article:in%20body%20link>, Zugriff am 12.12.2020.

Macaskill, E. & Dance, G., 2013. *The Guardian - NSA-Files decoded: What the revelations mean for you*. Verfügbar unter:

<https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>, Zugriff am 10.12.2020.

Marr, B., 2019. *Forbes - Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids?*. Verfügbar unter:

<https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/?sh=e54f15748b83>, Zugriff am 25.11.2020.

Mozur, P., 2018. *The New York Times - Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*. Verfügbar unter:

<https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>, Zugriff am 25.11.2020.

Mozur, P., Zhong, R. & Krolik, A., 2020. *The New York Times - In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags*. Verfügbar unter:

<https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>, Zugriff am 17.11.2020.

Noor, P., 2021. *The Guardian - Should we celebrate Trump's Twitter ban? Five free speech experts weigh in*. Verfügbar unter:

<https://www.theguardian.com/us-news/2021/jan/17/trump-twitter-ban-five-free-speech-experts-weigh-in>, Zugriff am 31.01.2021.

Norton Rose Fulbright, 2020. *Contact tracing apps in China: A new world for data privacy*.

Verfügbar unter: <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact->

tracing/china-contact-tracing.pdf?revision=249d55f4-eb9a-49dd-8491-b8c9c7626691&la=en-cn, Zugriff am 17.11.2020.

Olivia, S. & Laughland, O., 2018. *The Guardian - Cambridge Analytica closing after Facebook data harvesting scandal*. Verfügbar unter: <https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say>, Zugriff am 05.01.2021.

OpenNet, 2004. *OpenNet Initiative: Bulletin 005 – Probing Chinese Search Engine Filtering*. Verfügbar unter: <https://opennet.net/bulletins/005/>, Zugriff am 12.11.2020.

Reporters Without Borders, 2014. *Enemies of the Internet 2014 - Russia: Control from the top down*. Verfügbar unter: <https://www.refworld.org/docid/533925b45.html>, Zugriff am 08.12.2020.

Roose, K., 2021. *The New York Times - In Pulling Trump's Megaphone, Twitter Shows Where Power Now Lies*. Verfügbar unter: <https://www.nytimes.com/2021/01/09/technology/trump-twitter-ban.html>, Zugriff am 31.01.2021.

Rosenberg, M., Confessore, N. & Cadwalladr, C., 2018. *The New York Times - How Trump Consultants Exploited the Facebook Data of Millions*. Verfügbar unter: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>, Zugriff am 30.12.2020.

Shahbaz, A. & Funk, . A., 2020. *The Pandemic's Digital Shadow*. Verfügbar unter: <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow>, Zugriff am 06.11.2020.

State Council General Office , 2007. *Some Opinions concerning the Construction of a Social Credit System*. Verfügbar unter: <https://chinacopyrightandmedia.wordpress.com/2007/03/23/state-council-general-office-some-opinions-concerning-the-construction-of-a-social-credit-system/>, Zugriff am 20.11.2020.

State Council General Office, 2014. *Planning Outline for the Construction of a Social Credit System (2014-2020)*. Verfügbar unter: <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>, Zugriff am 20.11.2020.

Statista, 2020. *Angezeigte Fälle von Cybercrime (gesamt) in Österreich von 2004 bis 2019*. Verfügbar unter: <https://de.statista.com/statistik/daten/studie/294141/umfrage/cybercrime-in-oesterreich/>, Zugriff am 31.01.2021.

Statista, 2020. *Number of Internet users in China from December 2008 to March 2020*. Verfügbar unter: <https://www.statista.com/statistics/265140/number-of-internet-users-in-china/>, Zugriff am 16.11.2020.

Statista, 2020. *Ranking der 20 Länder mit der höchsten Lebensqualität nach dem Best Countries Ranking 2020*. Verfügbar unter:

<https://de.statista.com/statistik/daten/studie/732084/umfrage/top-20-der-laender-mit-der-hoechsten-lebensqualitaet-nach-dem-best-countries-ranking/>, Zugriff am 15.01.2021.

Torfox, A Stanford Project, 2011. *The Great Firewall of China: Background*. Verfügbar unter: <https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html>, Zugriff am 10.11.2020.

Trivium Social Credit, 2020. *Supreme People's Court grants leniency to support post-COVID work resumption*. Verfügbar unter: <http://socialcredit.triviumchina.com/2020/05/supreme-peoples-court-grants-corporate-leniency-to-support-post-covid-work-resumption/>, Zugriff am 25.11.2020.

Twitter Safety, 2021. *Twitter*. Verfügbar unter: <https://twitter.com/TwitterSafety/status/1346970430062485505>, Zugriff am 31.01.2021.

Twitter, 2021. *Civic Integrity Policy*. Verfügbar unter: <https://help.twitter.com/en/rules-and-policies/election-integrity-policy>, Zugriff am 31.01.2021.

Twitter, 2021. *Permanent suspension of @realDonaldTrump*. Verfügbar unter: https://blog.twitter.com/en_us/topics/company/2020/suspension.html, Zugriff am 31.01.2021.

Walker, S., 2013. *The Guardian - Russia to monitor 'all communications' at Winter Olympics in Sochi*. Verfügbar unter: <https://www.theguardian.com/world/2013/oct/06/russia-monitor-communications-sochi-winter-olympics>, Zugriff am 08.12.2020.

WKO, 2020. *China führt ab 2021 ein Social Credit System für Unternehmen ein*. Verfügbar unter: <https://news.wko.at/news/wien/China-fuehrt-ab-2021-ein-Social-Credit-System-fuer-Unterneh.html>, Zugriff am 06.11.2020.

Zeit Online, 2017. *Neues Anti-Terror-Gesetz statt Ausnahmezustand*. Verfügbar unter: <https://www.zeit.de/politik/ausland/2017-10/frankreich-antiterrorgesetz-ausnahmezustand-emmanuel-macron>, Zugriff am 15.01.2021.

Rechtsquellen

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSGVO)

StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.) [CELEX-Nr.: 395L0046]. Verfügbar unter: <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597>, Zugriff am 04.02.2021

Maßnahmen für die Verwaltung von Internet- und Informationsdiensteanbieter 2000, Dekret Nr. 292 des Staatsrats der Volksrepublik China, Verfügbar unter: <https://www.cecc.gov/resources/legal-provisions/measures-for-the-administration-of-internet-information-services-cecc>, Zugriff am 15.12.2020

Regulation of Investigatory Powers Act 2000 c. 23 (RIPA). Verfügbar unter: <https://www.legislation.gov.uk/ukpga/2000/23/contents>, Zugriff am 04.02.2021

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Verfügbar unter: <http://data.europa.eu/eli/reg/2016/679/oj>, Zugriff am 04.02.2021.

10. Abbildungsverzeichnis

Abbildung 1: CAP-Theorem	13
Abbildung 2: China vs U.S. Internet	19
Abbildung 3: Datensammlung und Bestrafung	24
Abbildung 4: Erfassung der Facebook-Daten	I