Arbeiterkammer Wien
Abteilung Konsumentenpolitik
Prinz-Eugen-Straße 20-22
A-1041 Wien
Tel: ++43-1-501 65/3136 DW
Fax: ++43-1-501 65/2693 DW
Internet: www.ak-konsumentenschutz.at
E-Mail: konsumentenpolitik@akwien.at

42/2014
November 2014

KOMMERZIELLE DIGITALE ÜBERWACHUNG IM ALLTAG

Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data: Internationale Trends, Risiken und Herausforderungen anhand ausgewählter Problemfelder und Beispiele.

Cracked Labs
Institut für Kritische Digitale Kultur

Cracked Labs – Institut für Kritische Digitale Kultur
http://crackedlabs.org

Projektleitung und Autor: Wolfie Christl

Studie im Auftrag der Bundesarbeitskammer

Oktober 2014

ISBN: **978-3-7063-0512-9**

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

Diese Studie basiert auf mehreren Jahren Forschungsarbeit, die größtenteils während der Entwicklung des kritisch-didaktischen Online-Spiels „Data Dealer“ erfolgt ist. Dieses *Serious Game* gilt inzwischen international als „Best Practice“ Projekt im Feld Datenschutz, Überwachung und Medienpädagogik. Die Zusammenfassung der Recherchen erfolgte zwischen Juli und Oktober 2014.

Ein unübersichtliches Themenfeld...

Ziel der Forschungsarbeit war es, einen umfassenden Blick darauf zu werfen, wie die Speicherung, Verknüpfung und Verwertung von digitalen persönlichen Daten heute im Detail funktioniert und welche gesellschaftlichen Implikationen sich daraus ergeben. Nicht zuletzt sollten Antworten auf die dringende Frage gefunden werden: Was tun? Diese Ziele konnten natürlich nicht vollständig erreicht werden. Dazu ist das Themenfeld nicht nur zu vielfältig und unübersichtlich, auch die Technologien und deren Anwendung verändern sich zu rasant. Wissenschaft und Forschung hinken der Entwicklung hinterher. Der Journalismus befasst sich zwar sowohl auf globaler als auch auf regionaler Ebene immer wieder mit Teilaspekten – aber meist nur kurzfristig und oberflächlich. Zivilgesellschaftliche Organisationen in den Feldern Datenschutz und digitale Rechte sind hoffnungslos unterbudgetiert. Selbst viele ExpertInnen sind schlicht und einfach etwas ratlos.

Drei Hauptkapitel

Trotzdem ist im Rahmen dieser Studie hoffentlich ein guter Überblick über die Thematik gelungen. Nach einem einleitenden Kapitel über Privatsphäre, Datenschutz, persönliche Daten und Überwachung folgen die drei Hauptkapitel: Nach einer Darstellung der inzwischen sehr weit gehenden Möglichkeiten der **Verknüpfung und Analyse persönlicher Daten** im Zeitalter von *Big Data* folgen ein Überblick über datenhungrige **Geräte und Plattformen** sowie ein Kapitel über die „Platzhirsche“ im **Handel mit persönlichen Daten.** Diese Einteilung beruht auf einer zweckmäßigen Differenzierung und ist ein guter Kompromiss - in der Praxis überschneiden und durchdringen sich die drei Felder. Die oft thematisierten großen Player *Google* und *Facebook* fehlen als eigene Gegenstände der Untersuchung – die beiden Unternehmen mussten aber dennoch oft genug erwähnt werden.

Eine grundsätzliche Anmerkung: Ich benutze aus Gründen der Lesbarkeit fast durchgehend den Begriff „persönliche Daten“ anstatt des juristisch korrekten Begriffs der „personenbezogenen Daten“.

Vielen Dank

Abschließend möchte ich mich beim Team vom „Data Dealer“ bedanken – und bei der Community rund um das Spiel. Dieses Projekt und die vielen Rückmeldungen sind die Basis dieser Forschungsarbeit. Insbesondere möchte ich Renée Winter danken, die nicht nur von Herbst 2012 bis Winter 2013 das Recherche-Wiki betreut hat, sondern auch in vielen Gesprächen zur Verfügung gestanden hat - genauso wie Severin Christl. Ein weiterer Dank gilt der österreichischen **Arbeiterkammer** und deren Unterstützung, **Walter Peissl** für Gedankenaustausch und insbesondere dessen Untersuchung des *Smartphone*-Universums[1], **Andreas Schumann** und dessen Recherchen über Adresshandel und Scoring in Deutschland[2] sowie **Anna Biselli** und ihrer Serie „How-To Analyze Everyone“[3]. Und all den anderen engagierten, tollen Menschen, die sich mit der Thematik intensiv beschäftigen, die ich auf Konferenzen und anderen Veranstaltungen treffen durfte - oder deren Texte ich gelesen habe.

Wolfie Christl, Wien, 13.10.2014

---

1 http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a63.pdf
2 http://safeaddress.wordpress.com
3 https://netzpolitik.org/?s=How-To+Analyze+Everyone

1 Aufgabenstellung und Methodik

"That's No Phone. That's My Tracker"[4]
New York Times, 2012

Persönliche Daten als neues Öl des Internets

Durch die rasante Weiterentwicklung der Informations- und Kommunikationstechnologien dringt die Erfassung persönlicher Daten und immer mehr in den Alltag ein. Unsere Vorlieben und Abneigungen werden heute in einem Ausmaß **digital gespeichert, verarbeitet und verwertet**, das bis vor wenigen Jahren undenkbar war. Laut der ehemaligen EU-Kommissarin für Verbraucherschutz Meglena Kuneva sind persönliche Daten „das neue Öl des Internets und die neue Währung der digitalen Welt"[5]. Einzelne Personen werden über Geräte und Plattformen hinweg wiedererkannt, deren Verhalten und Bewegungen detailliert ausgewertet, Persönlichkeit und Interessen akribisch analysiert. Ob via Kundenkarten, *Smartphones* oder im Netz – überall werden **digitalen Spuren** hinterlassen. Immer mehr Geräte sind heute mit Sensoren ausgestattet, mit dem Internet verbunden und ermöglichen so umfassende Einblicke in das Leben ihrer NutzerInnen. Gleichzeitig lassen sich im Zeitalter von *Big Data* mit automatisierten Methoden schon aus rudimentären Metadaten über Kommunikations- und Online-Verhalten umfangreiche Persönlichkeitsprofile erstellen.

Aufstrebende Firmen in den Feldern soziale Netzwerke, Online-Werbung, mobile *Apps* oder Fitness arbeiten mit Hochdruck an Geschäftsmodellen, die auf der **kommerziellen Verwertung der gesammelten Profile** beruhen. Internationale Unternehmen agieren dabei teils unter Missachtung regionaler Datenschutzgesetze, oft gilt die Devise: Gemacht wird, was technisch möglich ist. Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent – deren Services, *Apps*, Plattformen und Algorithmen sind zentralisiert und kaum durchschaubar. Darüber hinaus haben nicht nur die Enthüllungen von Edward Snowden gezeigt, dass auch **staatliche Behörden und Geheimdienste** gern auf die gesammelten Daten zugreifen. Die Privatsphäre ist heute gleichermaßen durch Unternehmen wie durch staatliche Behörden bedroht.

Diese Studie zielte darauf ab, anhand von **ausgewählten Problemfeldern und Beispielen** einen fundierten Überblick über internationale Trends in der zunehmenden Erfassung und Verwertung von persönlichen Daten durch Unternehmen zu geben und mögliche Auswirkungen auf die NutzerInnen zu beschreiben. Schlussendlich sollten Antworten auf folgende Fragen gegeben werden: In welcher Form könnte kommerzielle digitale Überwachung zukünftig den Alltag prägen? Was sind die Risiken – sowohl für die Gesellschaft als auch für Einzelne? Und welche Handlungsoptionen ergeben sich daraus für Politik, Öffentlichkeit, Unternehmen und BürgerInnen?

Forschungsmethodik

Die vorliegende Studie basiert auf **mehreren Jahren Forschungsarbeit** zum Thema und stützt sich auf systematische Literaturrecherche, Dokumentenanalyse, die gezielte Suche in internationalen Online-Archiven von Zeitungen und digitalen Medien sowie auf Webseiten von Unternehmen, Organisationen und Behörden. Darüber hinaus wurden in den letzten Jahren hunderte Gespräche auf Konferenzen, Veranstaltungen und via Skype geführt – mit ExpertInnen in den

4 Peter Maass, Megha Rajagopalan: That's No Phone. That's My Tracker. New York Times, 13.07.2012. Abgerufen am 10.07.2014 von http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html

5 Meglena Kuneva: Roundtable on Online Data Collection, Targeting and Profiling. European Commission Speech, 31.03.2009. Abgerufen am 14.09.2014 von http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm

Bereichen Datenschutz, Netzpolitik, Konsumentenschutz, IT-Sicherheit, Web-Technologie, *Big Data*, *Social Media*, Marketing, *Apps* und *Quantified Self*.

Quellenlage

Manche Themen konnten umfangreicher abgedeckt, manche auch nur angerissen werden. Viele Unternehmen agieren intransparent, die Quellenlage ist teils schlecht. Die Entwicklung geht rasant voran, die vorhandenen wissenschaftlichen und journalistischen Recherche-Ergebnisse beziehen sich manchmal auf Services oder Apps, die schon einige Jahre danach gar nicht mehr existieren. Teils sind die **Eigenaussagen der Unternehmen** die einzig vorhandenen Quellen. Diese Eigenaussagen von Unternehmen sind sicherlich mit Vorsicht zu genießen. Es ist allerdings von Vorteil, dass viele Unternehmen nicht nur in Richtung KonsumentInnen werben, sondern ihre Dienstleistungen auch in Richtung Unternehmens-KundInnen verkaufen müssen. Diese an andere Unternehmen gerichteten Informationen legen manchmal viel mehr offen, als in Richtung der KonsumentInnen kommuniziert wird.

2 Privatsphäre, Datenschutz und kommerzielle digitale Überwachung

„Wir leben im Computerstaat“[6]
Songtext der deutschen Band „Abwärts“, 1980

Schutz vor Datenmacht

Die Wurzeln des heutigen Konzepts von **Privatsphäre** werden meist in der Neuzeit verortet, wo nach Kai von Lewinski (2012) parallel zum Erstarken des Bürgertums gegenüber dem Adel, der Entstehung von Aufklärung, Humanismus, Liberalismus und Anarchismus sowie der Entdeckung des „Individuums“ auch der moderne Staat und dessen bürokratische Datenmacht entstand. Der Staat und später auch Unternehmen gewannen gegenüber dem Einzelnen ein „informationelles Übergewicht“. Daraus entstand das zentrale Motiv des **Datenschutzes** als „Schutz vor Datenmacht“ - und damit auch die Überzeugung, dass „informationelle Verhältnisse auch Machtbeziehungen“ sind und die Einzelnen vor „asymmetrischen Informationsbeziehungen“ geschützt werden müssten.

Mit dem Einsetzen verstärkter staatlicher Verwaltungs-Automatisierung und dem Aufkommen der ersten Großcomputer entstand in den 1960ern und 1970ern im deutschen Sprachraum eine neue Debatte über Privatsphäre – nicht zuletzt auch unter dem Eindruck des mörderischen Missbrauchs bürokratischer Datenmacht im Nationalsozialismus. 1970 verabschiedete das deutsche Bundesland Hessen international das **erste Datenschutzgesetz**, 1978 wurde das erste österreichische Datenschutzgesetz beschlossen (vgl. Tretter 2010).

Deutsche Volkszählung 1983

Mit den Protesten gegen die deutsche Volkszählung 1983 trat die Debatte in das Bewusstsein einer breiten Öffentlichkeit, angeheizt von den ersten automatisierten Rasterfahndungen und den Verschärfungen staatlicher Überwachung infolge von 1968er-Opposition und RAF-Terrorismus – und sicherlich mitgeprägt von der Rezeption von George Orwells Roman „1984“. Im sogenannten **Volkszählungsurteil** schuf der deutsche Bundesverfassungsgerichtshof erstmals das zuvor schon von Steinmüller konzipierte „Recht auf informationelle Selbstbestimmung“ (vgl. Pohle 2014).

2.1. Informationelle Selbstbestimmung, Datenschutz und personenbezogene Daten

Seit 1983 garantiert das deutsche **Grundrecht auf informationelle Selbstbestimmung**[7] den „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten“ und das Recht jedes Menschen, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ - und zwar „unter den Bedingungen der modernen Datenverarbeitung.“

Grundrecht auf Datenschutz

In Österreich bürgt der erste Satz im **Datenschutzgesetz 2000**[8] für ein Grundrecht auf Daten-

6 http://de.wikipedia.org/wiki/Computerstaat

7 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983 (1 BvR 209, 269, 362, 420, 440, 484/83). Abgerufen am 14.09.2014: http://www.bfdi.bund.de/DE/GesetzeUndRechtsprechung/Rechtsprechung/BDSGDatenschutzAllgemein/Artikel/151283_VolkszaehlungsUrteil.html

8 (Österreichisches) Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.). Online:

schutz: „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." Ein derartiges schutzwürdiges Interesse sei allerdings ausgeschlossen, wenn „Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind."

Zustimmung, Richtigstellung und Löschung

Die schutzwürdigen Geheimhaltungsinteressen einer betroffenen Person werden aber dann nicht verletzt, wenn eine „informierte Zustimmung" des Betroffenen vorliegt. Diese wird definiert als „gültige, insbesondere ohne Zwang abgegebene **Willenserklärung des Betroffenen**, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt." Darüber hinaus existiert ein „**Recht auf Auskunft** darüber, wer welche Daten [...] verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden" sowie ein „Recht auf **Richtigstellung unrichtiger Daten** und das **Recht auf Löschung** unzulässigerweise verarbeiteter Daten."

Personenbezogene Daten?

Außerdem werden im österreichischen Datenschutzgesetz folgende Begriffe definiert:

- **Personenbezogene Daten** sind Angaben über Betroffene, „deren Identität bestimmt oder bestimmbar ist"
- **Indirekt personenbezogene Daten** sind hingegen solche, bei denen „die Identität des Betroffenen mit rechtlich zulässigen Mitteln" nicht bestimmt werden kann
- **Sensible Daten** oder „besonders schutzwürdige Daten" sind „Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben"

Wie werden persönliche Daten definiert?

Alle anderen Daten sind keine personenbezogenen Daten und fallen als „anonyme" Daten nicht unter das Datenschutzgesetz, auch indirekt personenbezogene Daten sind schlecht geschützt. Bei indirekt personenbezogenen Daten kann zwar die Identität einer Person „mit rechtlich zulässigen Mitteln" nicht „bestimmt" werden – sehr wohl aber durch Dritte. Beispiele für indirekt personenbezogene Daten sind die **Sozialversicherungsnummer**, **KFZ-Kennzeichen** oder **Matrikelnummern an Universitäten**. Diese Daten können unter bestimmten Bedingungen auch ohne Zustimmung der Betroffenen verwendet werden (vgl. ARGE Daten 2006). Die Abgrenzung zwischen personenbezogenen, indirekt personenbezogenen und anonymen Daten ist umstritten, aber entscheidend für die Wirksamkeit eines Datenschutzgesetzes.

Nach Beate Rössler (2001) ist es **ethisch problematisch**, wenn persönliche Daten gegen den eigenen Willen und ohne das eigene Wissen weitergegeben werden – oder wenn Betroffene systematisch darüber getäuscht werden, welche Daten in welchem Ausmaß und in welchem Umfang an welche Dritten weitergegeben werden.

2.2. Datenschutzrechtliche Ausnahmeregelungen

Sowohl in Österreich als auch in Deutschland gelten Ausnahmeregelungen für bestimmte Arten der gewerblichen Nutzung persönlicher Daten.

Regelungen für Adressverlage und Direktmarketing

In **Österreich** existiert beispielsweise in Form von § 151 der Gewerbeordnung[9] eine Ausnah-

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597

9 § 151 GewO. Online: https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR40096343

meregelung für die Verwendung persönlicher Daten für „Marketingzwecke Dritter“ durch Adressverlage und Direktmarketingunternehmen, nach der „Kunden- und Interessentendateien“ mit Name, Geschlecht, Adresse, Geburtsdatum, Beruf und der „Zugehörigkeit des Betroffenen zu dieser Kunden- und Interessendatei“ in vielen Fällen auch ohne ausdrückliche Zustimmung der Betroffenen gewerblich weitergegeben werden können. Voraussetzung dafür ist, dass die Betroffenen von dem Unternehmen, das die Daten weitergibt, darüber informiert wurden, dass sie die „Übermittlung ihrer Daten für Marketingzwecke Dritter“ untersagen können. Außerdem dürfen einzelnen Personen durch „Marketinganalyseverfahren“ bestimmte Eigenschaften „zugeschrieben“ werden. Beispielsweise können aus Wohnadressen oder dem Alter bestimmte Wahrscheinlichkeiten für **Einkommensklassen** oder **Gesundheitsinteressen** berechnet werden[10]. Im Rahmen dieser Regelung dürfen im Prinzip unendlich viele Listen von Personen mit unterschiedlichen Eigenschaften verwaltet und weitergegeben werden.

Umstritten: Das deutsche „Listenprivileg“

Rechtliche Basis für den Adresshandel und andere Nutzungsarten persönlicher Daten in **Deutschland** ist das sogenannte **Listenprivileg**[11] - eine Ausnahmeregelung im deutschen Datenschutzrecht, die die Nutzung von personenbezogenen Daten zu Werbezwecken, zur Markt- und Meinungsforschung sowie die (gewerbliche) Weitergabe an Dritte erlaubt. Nach § 28[12] und § 29[13] des deutschen Bundesdatenschutzgesetzes dürfen Adresslisten mit Name, Anschrift, Geburtsjahr, Beruf und die „Zugehörigkeit der Betroffenen“ zu einer bestimmten „Personengruppe“ unter bestimmten Bedingungen verarbeitet, genutzt und übermittelt werden. Da die Anzahl der Listen nicht beschränkt ist, können durch die erwähnte Zugehörigkeit zu einer bestimmten Personengruppe eine Vielzahl an Listen mit jeweils anderen Eigenschaften erstellt werden. Eine Zustimmung der Betroffenen ist dazu nicht erforderlich, die Betroffenen können allerdings der Nutzung ihrer Daten widersprechen („Opt-out“). Diese umstrittene Ausnahmeregelung wurde 2009 beinahe abgeschafft, nach der heftigen Kritik von Verbänden im Bereich Marketing, Werbewirtschaft, Versandhandel, Zeitungs- und Zeitschriftenverlegern aber doch beibehalten. Der deutsche „Verbraucherzentrale Bundesverband“ tritt für eine Abschaffung des Listenprivilegs ein[14].

2.3. Europäische Union, USA und allgemeine Menschenrechtserklärung

Das österreichische Datenschutzgesetz 2000 ist die nationale Umsetzung der **EU-Datenschutzrichtlinie** von 1995, die Mindeststandards zum Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten beschreibt, die in allen Mitgliedsstaaten der Europäischen Union seit 1998 durch nationale Gesetze sichergestellt sein müssen. Der deutsche EU-Parlamentsabgeordnete Jan Philipp Albrecht bezweifelt das hingegen und diagnostiziert, dass durch die unterschiedlich strengen nationalen Umsetzungen derzeit geltendes EU-Recht nicht durchgesetzt würde (vgl. Albrecht 2014).

Europäische Datenschutz-Verordnung

Die EU-Datenschutzrichtlinie von 1995 soll in Zukunft durch eine europäische Datenschutzverordnung ersetzt werden, die im Vergleich zu einer „Richtlinie“ **in allen Mitgliedsstaaten in glei-**

10 Österreichische Datenschutzbehörde: Datenschutz und Direktwerbung. Abgerufen am 29.09.2014 von https://www.dsb.gv.at/site/8144/default.aspx

11 http://de.wikipedia.org/wiki/Listenprivileg

12 § 28 Dt. Bundesdatenschutzgesetz (BSDG): Datenerhebung und -speicherung für eigene Geschäftszwecke. Online: http://www.gesetze-im-internet.de/bdsg_1990/__28.html

13 § 29 Dt. Bundesdatenschutzgesetz (BSDG): Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung. Online: http://www.gesetze-im-internet.de/bdsg_1990/__29.html

14 Wilkens, Andreas (2009): Neues Datenschutzrecht droht zu scheitern. heise.de, 27.05.2009. Abgerufen am 10.07.2014 von http://www.heise.de/ct/meldung/Neues-Datenschutzrecht-droht-zu-scheitern-220133.html

cher Weise verbindlich gelten soll. Im März 2014 haben 621 von 653 Abgeordneten des EU-Parlaments in erster Lesung für einen von Berichterstatter Albrecht ausgehandelten Text gestimmt. Der „Rat der Europäischen Union" - also der aus VertreterInnen der Mitgliedsstaaten bestehende Ministerrat - hat noch keine gemeinsame Position. Erst wenn sich Parlament und Rat geeinigt haben, ist der Weg für die neue EU-Datenschutzverordnung frei (vgl. Albrecht 2014).

„Privacy" in den USA und Menschenrechtserklärung

In den **USA** gilt der 1890 veröffentlichte Aufsatz „The Right to Privacy"[15] als erste Deklaration eines „Right to be let alone", das allerdings „stark vom durch die eigenen vier Wände begrenzten Raum gedacht" ist (Lewinski 2012). Für personenbezogene Daten wird im angloamerikanischen Raum der Begriff ***Personally identifiable information***[16] (PII) verwendet.

Das Recht auf Privatsphäre findet sich auch im Artikel 12 der **Allgemeinen Erklärung der Menschenrechte**[17]: „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen."

15 http://en.wikipedia.org/wiki/Right_to_privacy
16 http://en.wikipedia.org/wiki/Personally_identifiable_information
17 Allgemeine Erklärung der Menschenrechte. Resolution 217 A (III) vom 10.12.1948. Online: http://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=ger

2.4. Kommerzielle digitale Überwachung

Überwachung ist nach Marit Hansen (2012) das „zielgerichtete Beobachten einer Aktion, eines Objekts oder einer Person (Überwachungsziel) und das damit verbundene Sammeln von Informationen". Überwachungstechnologien sind in Folge alle „informationstechnologischen Instrumente, die sich für diesen Zweck nutzen lassen". Der Begriff kann sich auf viele unterschiedliche Bereiche beziehen – auch auf die Überwachung von automatisierten Produktionsprozessen, Maschinen oder etwa Vulkanen. In dieser Studie sei explizit die Überwachung von Personen und deren Handlungen gemeint. Traditionell wird der Begriff für staatliche Überwachung verwendet - oft auch im Kontext von Videoüberwachung, Überwachung von MitarbeiterInnen oder etwa der Überwachung durch Detektive.

Was ist Überwachung?

David Lyon – einer der Pioniere der Überwachungsforschung - definiert Überwachung als fokussierte, systematische und laufende Aufmerksamkeit auf persönliche Details **zum Zweck der Einflussnahme**, der Führung, des Schutzes oder der Lenkung[18] (vgl. Lyon 2007). Überwachung sei **fokussiert**, weil sie auf das Individuum ausgerichtet ist – auch wenn dabei aggregierte oder öffentliche Daten als Hilfsmittel eingesetzt werden. Sie erfolge **systematisch**, weil absichtlich, vorsätzlich und unter Einsatz bestimmter Protokolle und Techniken – und nicht etwa zufällig oder spontan. Und Überwachung erfolge **laufend**, sie sei „normaler" Teil des Alltagslebens in „bürokratisch administrierten Gesellschaften", die auf Informationstechnologie basieren. Überwachung sei einerseits ein „Set aus Praktiken", verfolge aber andererseits „Zwecke". In den daraus entstehenden **Machtbeziehungen** seien die BeobachterInnen privilegiert.

Kommerzielle Überwachung?

Durch sein Buch „The Electronic Eye: The Rise of Surveillance Society" hat Lyon (1994) den Begriff **Überwachungsgesellschaft** mitgeprägt und das Konzept des **Social Sorting** beschrieben – also die ständige Klassifikation und Sortierung der Bevölkerung durch Informationstechnologie und Software-Algorithmen auf Basis persönlicher Daten. Dies hätte Auswirkungen auf individueller Wahlmöglichkeiten und Lebenschancen. Gesellschaftliche Gruppen würden unterschiedlich behandelt, es entstünde **diskriminierendes Potential**. Automatisiertes *Social Sorting* erzeuge subtile Reihungen, durch die manche KonsumentInnen, KundInnen und BürgerInnen gegenüber anderen privilegiert würden – etwa durch unterschiedliche Preise oder Wartezeiten – und manche würden überhaupt ausgeschlossen.

Aufzeichnung des Alltags

Zwanzig Jahre nach Erscheinen dieses Buchs sind 2014 viele der von Lyon beschriebenen Aspekte Realität. Im Zuge von Internet und Digitalisierung ist digitale Überwachung heute beinahe allgegenwärtig – sowohl durch staatliche Behörden als auch durch Unternehmen. Immer mehr Geräte und Sensoren zeichnen unsere Handlungen auf, Unternehmen in beinahe allen Sektoren arbeiten an Einsatzmöglichkeiten und Geschäftsmodellen auf Basis dieses permanenten Datenflusses. Die meist unter dem Begriff ***Big Data*** gefassten Technologien der automatisierten Analyse und Auswertung großer Datenmengen ermöglichen die Erstellung von Persönlichkeitsprofilen und die Klassifizierung von Individuen aus der Aufzeichnung ganz alltäglicher Verhaltensweisen, Vorlieben und Abneigungen.

In den folgenden Kapiteln soll ein Überblick über internationale Trends im Bereich der Speicherung, Analyse und Verwertung persönlicher Daten gegeben werden – und damit das Feld der kommerziellen digitalen Überwachung umrissen werden.

18 Übersetzung durch den Verfasser, im Original: „the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction"

3 Analyse und Verknüpfung digitaler persönlicher Daten

„Alle Daten sind Kreditdaten, wir wissen nur noch nicht, wie wir sie richtig einsetzen“[19]
Douglas Merrill, ehem. Chief Information Officer (CIO) bei Google, 2012

3.1. Big Data und Verhaltensprognosen mit Statistik und Data Mining

Im Zuge der Digitalisierung haben sich in den letzten Jahrzehnten sowohl Speicher- als auch Rechenkapazitäten vervielfacht. Vor allem seit der Jahrtausendwende werden digitale Daten auf einem viel höheren Niveau gespeichert, verarbeitet und analysiert als jemals zuvor.

Unscharfer Begriff

Der Begriff ***Big Data***[20] bezeichnet in Öffentlichkeit und Fachwelt einerseits die großen digitalen Datenmengen selbst, manchmal aber auch deren Analyse und Auswertung. Es gibt keine etablierte wissenschaftliche Definition für den Begriff, er ist unscharf und gilt als Schlagwort[21]. Nach einer Definition von *Gartner*[22] bezieht sich das „Big“ im Begriff *Big Data* auf die drei Dimensionen **volume** (Umfang, Datenmenge), **velocity** (Geschwindigkeit, mit der die Daten generiert und transferiert werden) und **variety** (Bandbreite der Datentypen und -quellen). Das Beratungsunternehmen *McKinsey* verwendet eine „absichtlich subjektive“ Definition und spricht von Datenbeständen, die mit „typischen Datenbanken“ nicht mehr erfasst, gespeichert, verwaltet und analysiert werden können (vgl. Manyika 2011). Welche Datenmenge als groß eingeschätzt wird, differiere je nach Sektor, vorhandener Software und Anwendungszweck von „einigen Dutzend Terabytes bis mehreren Petabytes“.

In der Wissenschaft wird die Verarbeitung großer digitaler Datenmengen seit den 1990er-Jahren als große Herausforderung diskutiert, u.a. in der Meteorologie (Klimamodelle), der Bioinformatik (Genom-Analyse), der Physik (Simulationen) oder der Astronomie. Heute ist die Erfassung, Analyse und Auswertung großer Datenmengen in vielen Bereichen an der Tagesordnung – von staatlicher Überwachung über soziale Netzwerke und der Internet-Suche bis zur Finanzwirtschaft. Im Feld der **Business Intelligence**[23] dienen derartige Analysen der besseren Umsetzung von Unternehmenszielen.

Wahrscheinlichkeiten statt präziser Zahlen

Nach Viktor Mayer-Schönberger vom *Oxford Internet Institute* macht *Big Data* aus „präzisen Zahlen Wahrscheinlichkeiten“ und bewirkt **drei große Umwälzungen** (vgl. Mayer-Schönberger et al 2013):

- Die nicht nur auf kleine Stichproben beschränkte Analyse sehr großer Datenmengen bezogen auf ein konkretes Problem oder eine bestimmte Fragestellung.
- Die Akzeptanz einer gewissen Unschärfe anstatt von Exaktheit.
- Der „wachsende Respekt“ für Korrelationen anstatt der Suche nach Kausalitäten.

---

19 Hardy, Quentin (2012): Just the Facts. Yes, All of Them. New York Times, 24.03.2012. Abgerufen am 10.07.2014 von http://www.nytimes.com/2012/03/25/business/factuals-gil-elbaz-wants-to-gather-the-data-universe.html

20 http://en.wikipedia.org/wiki/Big_data

21 Harford, Tim (2014): Big data: are we making a big mistake? Financial Times, 28.03.2014. Abgerufen am 14.09.2014 von: http://www.ft.com/intl/cms/s/2/21a6e7d8-b479-11e3-a09a-00144feabdc0.html#axzz3DK9IcAdI

22 Gartner IT Glossary: „Big data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making“. Abgerufen am 14.09.2014 von: http://www.gartner.com/it-glossary/big-data

23 http://de.wikipedia.org/wiki/Business_Intelligence

Statistische Zusammenhänge und Kausalität

Statistische Korrelationen machen eine Aussage über den Zusammenhang zwischen zwei verschiedenen Merkmalen, Ereignissen, Zuständen oder Funktionen - es muss allerdings keine kausale Wirkung zwischen beiden bestehen. Ein bekanntes Maß für die Stärke eines linearen Zusammenhangs zwischen zwei Merkmalen ist der Korrelationskoeffizient[24], der Werte zwischen -1 und 1 annehmen kann. Besteht kein Zusammenhang, ist der Wert 0. Bei einem Wert von -1 besteht ein stark negativer, bei einem Wert von 1 ein stark positiver Zusammenhang.

Ein Beispiel für eine starke negative Korrelation wäre der Zusammenhang zwischen der (zunehmenden) zurückgelegten Strecke im Auto und der (abnehmenden) Treibstoffmenge im Tank. In diesem Fall wissen wir, dass gleichzeitig eine Ursache-Wirkungs-Beziehung besteht – also ein kausaler Zusammenhang. Wird zwischen zwei Variablen eine statistische Korrelation festgestellt und daraus irrtümlich auf einen kausalen Zusammenhang geschlossen, wird dies als „Cum hoc ergo propter hoc"[25] bzw. als **Scheinkorrelation**[26] bezeichnet.

Muster erkennen und Verhalten vorhersagen

Im Zeitalter von *Big Data* werden immer häufiger statistische Methoden eingesetzt, um große Mengen an NutzerInnendaten zu analysieren, darin **Muster und Zusammenhänge** zu erkennen, und daraus - über die Ausgangsinformationen weit hinausgehende - Einschätzungen über die NutzerInnen oder Prognosen über deren zukünftiges Verhalten zu treffen. Die dabei genutzten Technologien und Methoden werden unter dem Begriff ***Data Mining***[27] zusammengefasst. Dabei wird meistens eine gewisse Unschärfe in Kauf genommen, die getroffenen Einschätzungen und Prognosen müssen nicht in jedem Fall richtig sein, man setzt auf Wahrscheinlichkeiten.

Data Mining

Data Mining ist nach Oscar H. Gandy ein Prozess, in dem versucht wird, Rohdaten in „Information" zu transformieren - die dann strategisch für die Ziele einer Organisation eingesetzt werden kann (vgl. Gandy 2006). *Data Mining* zielt darauf ab, bestimmte Verhaltensweisen und „Marker" zu identifizieren, die als zuverlässige Indikatoren für Zukunftsprognosen dienen. Diese Bemühungen sind vom Interesse an Risikominimierung oder -vermeidung geprägt. Auch wenn es etwa darum geht, die oft zitierten 20% der KundInnen zu identifizieren, die einem Unternehmen 80% der Profite bieten[28], kann dies aus einer Perspektive des **Risikomanagements** betrachtet werden.

Bei derartigen Analysen werden einerseits mathematisch-statistische Verfahren genutzt (z.B. Clusteranalyse, Klassifikation, Assoziationsanalyse, Regressionsanalyse), andererseits Technologien des **Machine Learning**[29] - also Computerprogramme, die „automatisch lernen, komplexe Muster zu erkennen und intelligente Entscheidungen zu treffen" (vgl. Han et al 2011).

24 http://de.wikipedia.org/wiki/Korrelationskoeffizient
25 http://de.wikipedia.org/wiki/Cum_hoc_ergo_propter_hoc
26 http://de.wikipedia.org/wiki/Scheinkorrelation
27 http://de.wikipedia.org/wiki/Data-Mining
28 http://en.wikipedia.org/wiki/Pareto_principle
29 http://de.wikipedia.org/wiki/Maschinelles_Lernen

3.2. Predictive Analytics: Ausgewählte Problemfelder und Beispiele

Die in den folgenden Kapiteln zusammengefassten Analyse- und Prognose-Möglichkeiten werden unter dem Begriff **Predictive Analytics**[30] diskutiert und sind nur eine kleine Auswahl. Die beschriebenen statistischen Zusammenhänge, Korrelationen und Schlussfolgerungen sind bis zu einem gewissen Grad zuverlässig und nachvollziehbar, geben aber trotzdem nur Wahrscheinlichkeiten an. Bei den behandelten Forschungsergebnissen handelt es sich um öffentlich zugängliche Studien – teils unter Mitwirkung von Unternehmen wie *Nokia* oder *Facebook*. Der Großteil derartiger Analysen sowie deren praktische Anwendung erfolgen aber durch Unternehmen, die ihre Analysen und Algorithmen weitgehend nicht offen legen.

3.2.1. Schwangerschaftsprognose durch Einkaufsverhalten bei „Target"

Eines der meistzitierten Beispiele über die Prognose von sensiblen persönlichen Informationen durch die Analyse digitaler Daten, die auf den ersten Blick nicht sehr aussagekräftig zu sein scheinen, ist der Fall der **US-Supermarktkette *Target*** und deren Versuch, schwangere Kundinnen durch ihr Einkaufsverhalten zu identifizieren. Wie Charles Duhigg in der New York Times[31] und in seinem Buch „Die Macht der Gewohnheit" (2012) berichtet hat, weist *Target* allen KundInnen intern eine Identifikationsnummer zu – egal ob sie mit Kreditkarte bezahlen, einen Gutschein verwenden, eine Umfrage ausfüllen, die Telefon-Hotline anrufen, eine E-Mail von *Target* öffnen oder deren Website besuchen. Alle Einkäufe und Interaktionen würden protokolliert und bei Bedarf auch mit zugekauften Informationen angereichert.

Gezielte Ansprache zum richtigen Zeitpunkt

Duhigg hat ausführlich mit einem Statistiker von *Target* gesprochen, dessen Abteilung die Aufgabe hat, das Verhalten der KundInnen zu analysieren und daraus Handlungsempfehlungen für die Steigerung der Umsätze abzuleiten. Zu den einfacheren Aufgaben gehörte etwa die Identifikation von Eltern mit Kindern, um ihnen vor Weihnachten Kataloge mit Spielzeug zusenden zu können. Oder die Identifikation von KundInnen, die im April Badeanzüge gekauft haben, um ihnen im Juli Gutscheine für Sonnencreme und im Dezember Werbung für Diät-Ratgeber zu schicken. Die zentrale Herausforderung wäre es allerdings gewesen, **wichtige Momente im Leben der KundInnen ausfindig zu machen**, in denen ihr Einkaufsverhalten flexibel und damit Werbung oder Gutscheine sehr effektiv werden – beispielsweise Schulabschluss, Heirat, Umzug oder Scheidung. Eine gezielte Ansprache zum richtigen Zeitpunkt könne in diesen Lebensphasen das Einkaufsverhalten oft auf Jahre verändern.

Geburtstermine vorhersagen

Einer der **lukrativsten Momente** sei die Geburt eines Kindes, denn das Einkaufsverhalten von frischgebackenen Eltern sei flexibler als zu beinahe jedem anderen Zeitpunkt ihres erwachsenen Lebens. Nach aufwändigen Analysen hätten sich 25 Produkte herausgestellt, deren Kauf die Erstellung einer Art von „Schwangerschafts-Prognose-Score" ermögliche und sogar erlaube, mit einer bestimmten Wahrscheinlichkeit den Geburtstermin zu prognostizieren. Es geht dabei nicht um Produkte wie Babykleidung oder Kinderwägen, die ganz offensichtlich auf eine nahe Geburt schließen lassen, sondern um bestimmte Mengen von bestimmten Hautlotionen, Seife, Watte, Waschlappen oder Nahrungsergänzungsmittel, die **in bestimmten Frequenzen und Zeitabständen** gekauft werden.

Verhalten beeinflussen

Waren die schwangeren Frauen erst einmal identifiziert, erhielten sie verschiedene Arten von individueller Werbung, Gutscheine oder andere Kaufanreize – und zwar nicht nur für Babybedarf, sondern auch für ganz andere Produkte, bei denen man herausgefunden hätte, dass sie

30 http://en.wikipedia.org/wiki/Predictive_analytics

31 Charles Duhigg: How Companies Learn Your Secrets. New York Times, 16.02.2012. Abgerufen am 14.09.2014 von http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

von frischgebackenen Müttern gerne gleich mitgekauft werden. Duhigg berichtet weiterhin von einer **Anekdote**, nach der sich ein noch nicht informierter Vater eines schwangeren Teenagers empört an *Target* gewendet und sich über die an seine Tochter gerichteten Gutscheine für Babykleidung beschwert haben soll. Er hätte *Target* vorgeworfen, seine viel zu junge Tochter zu einer Schwangerschaft motivieren zu wollen.

Unabhängig davon, ob diese Anekdote wahr ist, zeigt dieses Beispiel, wie Unternehmen heute persönliche Daten analysieren und dazu einsetzen, um **mit bestimmten Handlungen** das Verhalten ihrer KundInnen zu verändern.

3.2.2. Prognose von sensiblen Persönlichkeitseigenschaften aus Facebook-Likes

Was sich aus durchschnittlich 170 Likes errechnen lässt

Eine US-Studie hat belegt, dass rein aus einer Analyse der *Facebook-Likes* auf die **ethnische Zugehörigkeit, politische Einstellung, Religion, Beziehungsstatus, Geschlecht, sexuelle Orientierung oder Nikotin-, Alkohol** und **Drogenkonsum** von Personen geschlossen werden kann (vgl. Kosinskia et al 2013). Die Studie basiert auf Daten von 58.486 US-BürgerInnen, die mittels freiwilliger Nutzung der *Facebook-App myPersonality* [32] einerseits ihre demographischen Informationen zur Verfügung gestellt haben sowie an Umfragen und Persönlichkeitstests teilgenommen haben. Andererseits wurden deren *Likes* analysiert – also deren positive Zustimmung zu Online-Inhalten wie Fotos und Statusmeldungen, populären Websites und zu *Facebook*-Seiten in den Bereichen Produkte, Sport, Musik, Bücher oder Restaurants. Folgende persönlichen Eigenschaften konnten allein aus den durchschnittlich 170 *Likes* der NutzerInnen mit hoher Zuverlässigkeit prognostiziert werden, die mittels Persönlichkeitstests erhobenen Informationen diente als Vergleichsbasis:

Prognostizierte Eigenschaft	Prognosezuverlässigkeit
Single oder in einer Beziehung	67%
Waren die Eltern im Alter von 21 noch zusammen?	60%
RaucherIn?	73%
Trinkt Alkohol?	70%
Konsumiert Drogen?	65%
Kaukasisch oder Afro-AmerikanerIn?	95%
Christlich oder muslimisch?	82%
Liberal oder konservativ?	85%
Schwul?	88%
Lesbisch?	75%
Geschlecht	93%

Tabelle 1: *Prognose persönlicher Eigenschaften aus Facebook-Likes. Quelle: Kosinskia et al, 2013.*

Keine offensichtlichen Schlüsse

Diese dichotomen Eigenschaften (ja/nein) wurden mit dem statistischen Verfahren der logistischen Regression[33] berechnet. Zusätzlich konnten mit dem Verfahren der linearen Regression[34] numerische Variablen wie etwa das **Alter** (zu 75%) oder die **Anzahl der Facebook-Freunde** (zu 47%) richtig prognostiziert werden. Wichtig ist dabei, dass nur wenige NutzerInnen Likes aufgewiesen haben, die ganz offensichtlich auf die jeweiligen Eigenschaften hindeuten. Beispielswei-

32 http://www.mypersonality.org/wiki (Abgerufen am 14.09.2014)
33 http://de.wikipedia.org/wiki/Logistische_Regression
34 http://de.wikipedia.org/wiki/Lineare_Regression

se waren weniger als 5% der als „schwul“ klassifizierten NutzerInnen mit explizit darauf hinweisenden *Facebook*-Gruppen wie z.B. „Being Gay“, „Gay Marriage“ oder „I love Being Gay“ verbunden. Die Prognosen basieren vielmehr auf weniger offensichtlichen, aber populäreren Vorlieben wie „Britney Spears” oder „Desperate Housewives” - die sich beispielsweise beide als schwache Indikatoren für männliche Homosexualität herausgestellt haben. Erstaunlicherweise konnte sogar für die Frage, ob sich die Eltern der NutzerInnen getrennt haben, bevor diese 21 Jahre alt wurden, eine Prognose-Zuverlässigkeit von 60% nachgewiesen werden.

Viele ähnliche Arten persönlicher Daten

Die Studie zeigt, dass aus der Analyse relativ rudimentärer Daten zum Online-Verhalten relativ zuverlässig und sehr weitgehend persönliche Eigenschaften abgeschätzt werden können, die üblicherweise als privat betrachtet werden. *Likes* repräsentieren eine generische Klasse von digitalen persönlichen Daten – strukturell ähnlich wie **Internet-Suchanfragen**, **Browser-Historien** oder **Kreditkartenzahlungen**. *Facebook-Likes*, die sich auf musikalische Vorlieben beziehen, bieten potenziell einen ähnlichen Informationsgehalt wie online **angehörte Songs**, **gekaufte Produkte** oder wie KünstlerInnen, nach denen online gesucht wurde. *Facebook-Likes* sind allerdings im Gegensatz zu diesen Informationen grundsätzlich für alle öffentlich zugänglich. Aber auch die anderen erwähnten Informationen sind teils für Dritte zugänglich (z.B. Suchmaschinen-Anbieter, Anbieter von *Facebook-Apps*, staatliche Überwachung) und es ist unwahrscheinlich, dass derartige Prognosemöglichkeiten auf die *Facebook*-Umgebung beschränkt sind.

Die *Facebook-App myPersonality*, mit der die *Likes* erfasst und die Umfragen und Persönlichkeitstests durchgeführt wurden, ist noch immer online. Inzwischen haben über **7,5 Millionen Menschen** aus vielen Ländern teilgenommen, die Daten aus der *App* wurden bis heute in 39 Studien eingesetzt.

3.2.3. Prognose von Charaktereigenschaften aus Mobiltelefon-Metadaten

„Big Five“[35] bzw. das Fünf-Faktoren-Modell ist eines der führenden Modelle der Persönlichkeitspsychologie[36] und wurde allein zwischen 1999 und 2006 in fast 2.000 wissenschaftlichen Studien erwähnt.[37] Viele Studien belegen die Reproduzierbarkeit und Konsistenz des Modells über verschiedene Altersgruppen und Kulturen hinweg. Daneben gibt es auch Stimmen, die die Aussagekraft und Genauigkeit des Modells anzweifeln oder dessen mangelnde theoretische Fundierung oder die ausschließliche Fokussierung auf das statistische Verfahren der Faktorenanalyse kritisieren.[38] Unabhängig davon wurde das Modell in den letzten Jahren aber oft im Zusammenhang mit der **Prognose von Charaktereigenschaften aus digitalen Daten** eingesetzt.

Das „Big Five“ Modell

Nach dem „Big Five“-Modell lässt sich jede Person auf folgenden fünf Skalen einordnen[39]:

Eigenschaft	Beschreibung
Neurotizismus	Personen mit hohen Werten in der Skala „Neurotizismus“ neigen dazu, nervös, ängstlich,

35 http://de.wikipedia.org/wiki/Big_Five_(Psychologie)

36 McCrae, R. R.; John, O. P. (1992): An introduction to the five-factor model and its applications. Journal of Personality, 60:175-215, 1992. Abgerufen am 14.09.2014 von: http://www.workplacebullying.org/multi/pdf/5factor-theory.pdf

37 John, Oliver P.; Naumann, Laura P.; Soto, Christopher J. (2008): Paradigm Shift to the Integrative Big Five Trait Taxonomy. Handbook of Personality Theory and Research. 3. Auflage. S. 114-117. Abgerufen am 14.09.2014 von: http://www.ocf.berkeley.edu/~johnlab/2008chapter.pdf

38 Block, Jack (2010): "The five-factor framing of personality and beyond: Some ruminations". Psychological Inquiry 21 (1): 2–25. Abgerufen am 14.09.2014 von: http://psychology.okstate.edu/faculty/jgrice/psyc4333/Block_Jack_2010.pdf

39 Beschreibungen nach: Borkenau, P. & Ostendorf, F. (2008). NEO-Fünf-Faktoren Inventar nach Costa und McCrae (NEO-FFI). Manual (2., neu normierte und vollständig überarbeitete Auflage). Göttingen: Hogrefe.

	traurig, unsicher und verlegen zu sein und sich Sorgen um ihre Gesundheit zu machen. Sie neigen zu unrealistischen Ideen und sind weniger in der Lage, ihre Bedürfnisse zu kontrollieren und auf Stresssituationen angemessen zu reagieren.
Extraversion	Personen mit hohen Werten in der Skala „Extraversion" sind gesellig, aktiv, gesprächig, personenorientiert, herzlich, optimistisch und heiter. Sie mögen Anregungen und Aufregungen.
Offenheit für Erfahrungen	Personen mit hohen Werten in der Skala „Offenheit für Erfahrung" zeichnen sich durch eine hohe Wertschätzung für neue Erfahrungen aus, bevorzugen Abwechslung, sind wissbegierig, kreativ, phantasievoll und unabhängig in ihrem Urteil. Sie haben vielfältige kulturelle Interessen und interessieren sich für öffentliche Ereignisse.
Verträglichkeit	Personen mit hohen Werten in der Skala „Verträglichkeit" sind altruistisch, mitfühlend, verständnisvoll und wohlwollend. Sie neigen zu zwischenmenschlichem Vertrauen, zur Kooperativität, zur Nachgiebigkeit, und sie haben ein starkes Harmoniebedürfnis.
Gewissenhaftigkeit	Die Skala „Gewissenhaftigkeit" unterscheidet ordentliche, zuverlässige, hart arbeitende, disziplinierte, pünktliche, penible, ehrgeizige und systematische von nachlässigen und gleichgültigen Personen.

Tabelle 2: *Die fünf Charaktereigenschaften im „Big Five"-Persönlichkeitsmodell (NEO-FFI nach Costa und McCrae)*

Schweizer Studie

Nun hat eine Schweizer Studie in Zusammenarbeit mit *Nokia Research* nachgewiesen, dass „Big Five" Charaktereigenschaften mit einer **Genauigkeit von bis zu 75,9%** rein aus *Smartphone*-Metadaten abgeschätzt werden können (vgl. Chittaranjan et al 2011). Dabei wurden 83 Personen darum gebeten, sich mit einem Fragebogen selbst einzuschätzen. Gleichzeitig wurde acht Monate lang deren Kommunikationsverhalten mit einer speziellen *App* überwacht, u.a. wurden folgende Daten aufgezeichnet:

Kategorie	Welche Daten wurden erfasst und ausgewertet?
App-Nutzung	Anzahl der Nutzung folgender Apps: Office, Internet, Video/Audio/Music, Maps, Mail, YouTube, Kalender, Kamera, Chat, SMS, Spiele
Anrufe	Anzahl eingehende/ausgehende/versäumte Anrufe, Anzahl angerufene/anrufende Kontakte, durchschnittliche Dauer eingehende/ausgehende Anrufe
SMS	Anzahl empfangene/gesendete SMS, Anzahl EmpfängerInnen/SenderInnen, durchschnittliche Wortlänge
Bluetooth (BT)	Anzahl und Häufigkeit von BT IDs, wie oft wurde häufigste BT ID gesehen, maximale Dauer einer BT ID,...

Tabelle 3: *Ausgewertete Mobiltelefon-Nutzungsdaten. Quelle: Chittaranjan et al, 2011.*

Smartphone-Nutzung und Charakter

Es handelt sich dabei ausschließlich um sogenannte ***Metadaten***[40], nicht etwa um Kommunikationsinhalte. Durch statistische Regressionsanalyse konnten folgende **Zusammenhänge zwischen *Smartphone*-Metadaten und Charaktereigenschaften** festgestellt werden (anstatt „Neurotizismus" wurde umgekehrt „emotionale Stabilität" verwendet):

Smartphone-Nutzung		Emotionale Stabilität	Extraversion	Offenheit für Neues	Gewissenhaftigkeit	Soziale Verträglichkeit
Häufigere App-Nutzung von:	Office	- 0,23		- 0,26		- 0,18
	Kalender	- 0,16		- 0,18		- 0,18
	Internet		- 0,26	- 0,15		
	Kamera		- 0,15			
	Video/Audio/Music				-0,18	
Höhere Anzahl eingehender Anrufe		- 0,15	0,13			
Längere Dauer eingehender Anrufe			0,18	0,12		
Mehr versäumte Anrufe				- 0,12		
Höhere Anzahl angerufener Kontakte						0,17
Höhere Anzahl von SMS-EmpfängerInnen				- 0,13		- 0,13
Höhere durchschnittliche Wortlänge gesendeter SMS		0,14	- 0,15			

Tabelle 4: *Korrelationskoeffizienten **r** für Zusammenhänge zwischen Smartphone-Nutzung und Charaktereigenschaften mit p < 0,01. Quelle: Chittaranjan et al, 2011.*

Mangelnde emotionale Stabilität?

Die Tabelle zeigt, wie sich aus verschiedenen *Smartphone*-Nutzungsdaten wie etwa der Anzahl von Anrufen oder SMS mit einer bestimmten Wahrscheinlichkeit auf bestimmte Charaktereigenschaften schließen lässt. Beispielsweise wurde festgestellt, dass bei häufigerer Nutzung der „Office"-*App* die Wahrscheinlichkeit höher ist, dass die entsprechende NutzerIn weniger emotional stabil (r=0,23), weniger offen (r=0,26) und weniger sozial verträglich (r=0,18) ist. Bei Korrelationskoeffizienten < 0,5 sind die Zusammenhänge zwar schwach ausgeprägt, aber doch vorhanden.

NutzerInnen einschätzen

Außerdem wurde ein „Machine Learning"-Modell zur **automatisierten Klassifikation von NutzerInnen** auf Basis ihrer *Smartphone*-Metadaten entwickelt. In Summe konnte mit relativ hoher Zuverlässigkeit rein aus *Smartphone*-Metadaten prognostiziert werden, ob die fünf Charaktereigenschaften bei einer Person höher oder niedriger ausgeprägt sind:

Ist untenstehende Eigenschaft a) höher oder b) niedriger ausgeprägt?	Baseline	Prognosezuverlässigkeit
Emotionale Stabilität	52,2 %	71,5 %
Extraversion	58,6 %	75,9 %
Offenheit	59,0 %	69,3 %
Gewissenhaftigkeit	62,2 %	74,5 %
Verträglichkeit	58,4 %	69,6 %

Tabelle 5: *Prognose von Charaktereigenschaften aus Smartphone-Metadaten. Quelle: Chittaranjan et al, 2011.*

Gute Prognosezuverlässigkeit

Rein aus *Smartphone*-Metadaten konnte mit einer **Zuverlässigkeit von 70 bis 75% auf den Charakter** der analysierten Personen geschlossen werden. Der Wert in der Spalte „Baseline"

40 http://de.wikipedia.org/wiki/Metadaten

gibt die Wahrscheinlichkeit an, die höhere oder niedrigere Ausprägung einer Charaktereigenschaft bei einer Person zu „erraten", indem immer die häufigere Ausprägung gewählt wird[41]. Die Verbesserung der Prognosezuverlässigkeit durch die Einbeziehung von *Smartphone*-Metadaten im Vergleich zum „Erraten" ist augenscheinlich.

MIT-Studie

Eine andere Studie am *Massachusetts Institute of Technology* (vgl. Montjoye 2013) hat sich bei der Wahl der Datengrundlagen noch weiter beschränkt und verwendet nur Daten, die jeder Mobilfunk-Netzbetreiber in den sogenannten **Call Data Records** (CDR)[42] über alle KundInnen zur Abrechnung aufzeichnet bzw. die auch im Rahmen der staatlichen Vorratsdatenspeicherung zur Verfügung stehen. Die Studie basiert auf dem *Smartphone*-Verhalten von 69 US-TeilnehmerInnen, deren Daten 14 Monate aufgezeichnet wurden. Die Rohdaten wurden in Bezug auf Kriterien in 4 Bereichen aufbereitet:

Kategorie	Ausgewertete Daten
Regelmäßigkeit	z.B. Durchschnittlicher Zeitabstand zwischen Anrufen/SMS, Varianz
Diversität	z.B. Anzahl und Entropie der Kontakte, Verhältnis Kontakte zu Interaktionen
Bewegung	z.B. Täglich zurückgelegte Distanz, Anzahl und Entropie der besuchten Orte
Proaktivität	z.B. Anteil selbst initiierter Kommunikation, Antwortrate auf Anrufe/SMS

Tabelle 6: *Ausgewertete Mobiltelefon-Nutzungsdaten. Quelle: Montjoye, 2013.*

Differenziertere Einschätzung

Danach wurden wieder statistische Modelle entwickelt, die eine **dreistufige Prognose** der Anteile der fünf Charaktereigenschaften ermöglichen - und in Folge die automatisierten Prognosen mit den Ergebnissen klassischer Persönlichkeitstests verglichen:

Ist folgende Eigenschaft a) niedrig b) mittel c) hoch ausgeprägt?	Baseline	Prognosezuverlässigkeit
Neurotizismus	38%	63%
Extraversion	39%	61%
Offenheit	38%	49%
Gewissenhaftigkeit	36%	51%
Verträglichkeit	36%	51%

Tabelle 7: *Prognose von Charaktereigenschaften aus Mobiltelefon-Nutzungsdaten. Quelle: Montjoye, 2013.*

Die Studie zeigt, dass rein aus Mobilfunk-Daten mit relativ hoher Zuverlässigkeit Charaktereigenschaften abgeschätzt werden können. Die Prognoseergebnisse sind im Schnitt **um 42% besser als bei zufälliger Schätzung**. Die Prozentanteile bei „Baseline" beziehen sich wieder auf den Versuch, die drei möglichen Ausprägungen der Charakter-Anteile (niedrig, mittel oder hoch) durch Wahl der häufigsten Ausprägung zufällig zu „erraten".

Öffentliche Twitter-Profile

Eine weitere Studie hat sich mit der Prognose von Charaktereigenschaften aus rudimentären **Twitter-Metadaten** beschäftigt (vgl. Quercia et al 2011). Dabei wurden ebenfalls keinerlei Inhalte ausgewertet, als Basis dienten ausschließlich drei öffentlich zugängliche Werte: Anzahl *Followers*, Anzahl *Following*, Anzahl der Listen[43]. Die „Big Five"-Prognosen sind wie zu erwarten nicht sehr genau. Es ist trotzdem erstaunlich, dass die mittlere quadratische Abweichung (auf einer [1-5] Skala) immer noch unterhalb von 0,88 bleibt. Dabei zeigt sich, dass sich sogar aus einer äußerst geringen Anzahl von Datenpunkten Prognosen erstellen lassen. Derartige Prognosen sind vor allem dann gut einsetzbar, wenn sie in Modelle mit vielen anderen Variablen einfließen.

---

41 Beispiel: Wenn die Eigenschaft „Extraversion" bei einer höheren Anzahl von NutzerInnen „niedrig" ausgeprägt ist, wird immer die Ausprägung „niedriger" geraten.

42 http://de.wikipedia.org/wiki/Call_Detail_Record

43 Anzahl der „Listen", in denen Twitter-NutzerInnen Teil sind. Vgl.: https://support.twitter.com/articles/76460-using-twitter-lists (Abgerufen am 20.09.2014)

3.2.4. Analysen von besuchten Websites und Suchmaschinen-Nutzung

Mehrere Untersuchungen haben sich damit befasst, wie sich aus der Analyse besuchter Websites oder der Suchbegriffe auf die Persönlichkeit von anonymen NutzerInnen schließen lässt.

Charakterprofile von Websites

An der Universität Cambridge wurde etwa in Kooperation mit *Microsoft Research* eine Studie zum Thema „Persönlichkeit und Website-Wahl" durchgeführt, die Zusammenhänge zwischen besuchten Websites und wiederum den „Big Five" festgestellt hat (vgl. Kosinski et al 2012). Mehr als 160.000 NutzerInnen wurden untersucht, die Datenbasis stammt aus der bereits erwähnten *Facebook-App myPersonality*. Als eines der Ergebnisse ergaben sich durchschnittliche **„Big Five"-Profile für Tausende von Websites**. Hier zum Beispiel von drei in Bezug auf die Zielgruppe eng verwandten Seiten aus dem Bereich Kunst und „Do it yourself", bei denen die durchschnittlichen „Big Five"-Profile der BesucherInnen der Seite stark korrelieren:

Domain	Offen-heit	Gewissen-haftigkeit	Extra-version	Verträglich-keit	Neuroti-zismus	Analysierte Personen	Standard-abweichung
deviantART.com	0,4	0,19	0,42	- 0,05	0,16	3.154	+/- 0,01 - 0,02
Tumblr.com	0,23	- 0,23	-0,16	- 0,1	0,22	639	+/- 0,03
Etsy.com	0,41	0,14	-0,26	0,07	0,1	612	+/- 0,03

***Tabelle 8:** „Big Five"-Profile von durchschnittlichen BesucherInnen dreier Websites. Quelle: Kosinski et al, 2012.*

Auf den Charakter schließen

Wenn bei vielen Websites die durchschnittlichen „Big Five"-Werte der BesucherInnen bekannt sind, können diese dazu eingesetzt werden, aus den von „anonymen" NutzerInnen besuchten Website automatisiert auf deren Charakter zu schließen – ohne für eine derartige Einschätzung weitere Informationen einzubeziehen.

Alter und Geschlecht

Eine weitere Studie von *Microsoft Research* auf Basis von *myPersonality* hat 133 Millionen Suchanfragen von 3,3 Millionen NutzerInnen der Suchmaschine *Bing* untersucht (vgl. Bi et al 2013). Dabei konnte das **Alter** der NutzerInnen rein aus den Suchanfragen mit **74% Zuverlässigkeit** abgeschätzt werden - und das **Geschlecht** sogar mit **80% Zuverlässigkeit**. Auch die **religiöse und politische Einstellung** konnte mit einer relativ hohen Genauigkeit prognostiziert werden.

Bildungsgrad und Beruf

Eine belgische Studie hat sich mit der Vorhersage von demographischen Eigenschaften wie **Geschlecht**, **Alter**, **Bildungsgrad** und **beruflicher Tätigkeit** aus anonymen Webserver-Log-Dateien befasst (vgl. De Bock 2010). Dabei nahmen 4.338 NutzerInnen an einer Online-Umfrage teil, parallel dazu wurde deren Klickverhalten aus den Log-Dateien von 260 assoziierten belgischen Websites extrahiert. Bezüglich Klickverhalten wurden u.a. besuchte Websites, Seitenaufrufe, Besuchsfrequenzen, Dauer der Besuche, Uhrzeiten und Wochentage ausgewertet. Nach einer Training- und einer Scoring-Phase konnten eine relativ gute Prognosezuverlässigkeit erreicht werden:

Eigenschaft	Mögliche Werte	Fehlerrate bei Prognose
Geschlecht	Männlich, weiblich	4,94 – 6,23 %
Alter	12-17,18-24, 25-34, 35-44, 45-54, 55 und älter	2,92 – 4,05 %
Beruf	Top Management, Mittleres Management, Bauer/Handwerker/Kleinunternehmer, Angestellte/r, Arbeiter/in, Hausfrau/-mann, Pensionist/in, Arbeitslos, Student/in, Andere	1,99 – 3,01 %
Ausbildung	Keine/Grundschule, Lower Highschool, Highschool, College, Universität	2,56 – 4,03 %

***Tabelle 9:** Prognose von Geschlecht, Alter, Bildungsgrad und Beruf bei anonymen Website-BesucherInnen. Quelle: De Bock 2010.*

Bei der angegebenen Fehlerrate handelt es sich um den durchschnittlichen absoluten Fehler bei der Einschätzung in Prozent. Um zu vermeiden, dass Verzerrungen durch von mehreren Personen gemeinsam genutzte Computer auftreten, wurde in der Online-Umfrage explizit danach gefragt.

3.2.5. Prognose von Emotionen aus der Tastatur-Eingabedynamik

Eine kanadische Studie hat sich damit befasst, wie sich emotionale Zustände aus **Rhythmus und Dynamik** des Tippens auf einer Tastatur erkennen lassen (vgl. Epp et al 2011). Dabei wurden 12 TeilnehmerInnen durchschnittlich 4 Wochen lang mit einer Software überwacht, die jeden Tastendruck aufgezeichnet hat – und je nach Aktivität immer wieder ein kurzer Fragebogen eingeblendet, in dem der aktuelle emotionale Zustand abgefragt wurde.

Rhythmus und Tipp-Dynamik

Bei den Tastendruck-Ereignissen wurden jeweils die Zeitpunkte des Drückens und des Loslassens aufzeichnet, die Ereignisse in Folge in mehrere Zweibuchstaben- (z.B. „ab“, „cd“, „ef“,...) und Dreibuchstaben-Kombinationen (z.B. „asd“, „sdf“,...) zerlegt und unter anderem auf folgende Art gruppiert:

Zweibuchstaben-Kombinationen	Dreibuchstaben-Kombinationen
Zeitabstand zwischen Taste-1-gedrückt und Taste-2-gedrückt	Zeitabstand zwischen Taste-1-gedrückt und Taste-2-gedrückt
Zeitabstand zwischen Taste1-gedrückt und Taste-1-losgelassen	Zeitabstand zwischen Taste-2-gedrückt und Taste-3-gedrückt
Zeitabstand zwischen Taste1-losgelassen und Taste-2-gedrückt	Zeitabstand zwischen Taste-1-gedrückt und Taste-3-losgelassen
Anzahl der Zweibuchstaben-Ereignisse	Anzahl der Dreibuchstaben-Ereignisse

Tabelle 10: *Ausgewertete Tastatureingabe-Ereignisse. Quelle: Epp et al, 2011.*

Löschtaste und Sonderzeichen

Zusätzlich wurden „inhaltliche“ Variablen wie die **Anzahl der Fehler** (*Backspace*- und *Delete*-Taste) oder der prozentuelle Anteil der Sonderzeichen (Ziffern, Interpunktion, ...) aufbereitet. Längere Pausen, Unterbrechungen oder Maus-Nutzung wurde exkludiert. Nach einer Klassifikationsphase mit mehreren selbstlernenden Modellen konnten schließlich folgende Erfolgsraten bei der Prognose von Emotionen aus der Tastatur-Eingabedynamik erzielt werden:

Zuversicht	Unschlüssigkeit	Nervosität	Entspannung	Trauer	Müdigkeit
83%	82%	83%	77%	88%	84%

Tabelle 11: *Zuverlässigkeit der Prognose von Emotionen aus der Tastatur-Eingabedynamik. Quelle: Epp et al, 2011.*

Es handelt sich dabei um dichotome Prognosen (z.B. „Zuversicht“ ja oder nein), die Prognosezuverlässigkeit liegt mit **zwischen 77% und 88%** weit über der Wahrscheinlichkeit bei zufälligem Raten (50%). Die Studie zeigt, dass sich rein aus dem Tippverhalten Prognosen über emotionale Zustände errechnen lassen, die mit der Eigenwahrnehmung der NutzerInnen gut übereinstimmen.

3.2.6. Vorhersage zukünftiger Aufenthaltsorte durch Smartphone-Daten

…ich weiß, wo du morgen sein wirst

Ein britisches Forschungsteam konnte auf Basis zeitlich zurückliegender GPS- und WLAN-Protokolle, Telefonnummern, Anruf- und SMS-Listen von 25 TeilnehmerInnen einer Studie deren Aufenthaltsorte zu einem Zeitpunkt **24 Stunden später** mit einer hohen Genauigkeit vorhersagen (vgl. De Domenico et al 2012).

Bei der Vorhersage des Aufenthaltsorts rein auf Basis der Daten einzelner TeilnehmerInnen lag

Einbeziehung der Daten von Bekannten

der durchschnittliche Fehler bei **1000 Metern**. Wenn allerdings nicht nur die Daten von einzelnen TeilnehmerInnen, sondern auch die von denjenigen berücksichtigt wurden, die mit den jeweiligen TeilnehmerInnen interagierten, konnte der durchschnittliche Fehler bei der Vorhersage bis auf **20 Meter** reduziert werden. Die **Verhaltensmuster von Bekannten korrelieren teils miteinander** und können darum dabei helfen, die Vorhersagen schwer vorhersehbarer Verhaltensmuster massiv zu verbessern. Der Algorithmus kann bei dieser Fehlerrate zwar immer noch manchmal völlig falsch liegen, aber die Wahrscheinlichkeit für eine richtige Prognose ist relativ hoch.

Der Studienautor gibt im Interview[44] mit *MIT Technology Review* zu bedenken, dass die TeilnehmerInnen nicht die Gesamtbevölkerung repräsentieren, da alle als Studierende und WissenschafterInnen in einem 30-Meilen-Radius um Lausanne leben und darum deren Bewegungsradius leichter vorhersehbar ist. Nichtsdestotrotz bleibt auf jeden Fall die Erkenntnis, dass die Berücksichtigung sozialer Netzwerke bei der Analyse von Verhaltensmustern die daraus abgeleiteten Prognosen hochgradig zuverlässiger machen kann.

Einsatzmöglichkeiten

Derartige Vorhersagen zukünftiger Aufenthaltsorte könnten einerseits für kommerzielle Zwecke eingesetzt werden – beispielsweise durch eine Platzierung von Anreizen in Form von **Werbung oder Rabatten** genau zum richtigen Zeitpunkt. Andererseits wäre auch ein Einsatz seitens **staatlicher Behörden** denkbar. Hier könnte beispielsweise umgekehrt ein besonderes Augenmerk darauf gelegt werden, welche Bewegungen **nicht der Prognose** entsprechen. Sogar ein Verzicht auf GPS-Daten wäre denkbar, beim Einsatz derartiger Algorithmen auf Basis von Bewegungs-Daten über die Funkmasten von Mobilfunk-Netzbetreibern wäre allerdings die Genauigkeit geringer.

3.2.7. Vorhersage von Beziehungen und Trennungen aus Facebook-Daten

Eine Studie unter Beteiligung des Unternehmens *Facebook* hat 2013 die Daten von **1,3 Millionen** zufällig ausgewählten ***Facebook*-NutzerInnen** mit zwischen 50 und 2000 „Friends" untersucht, die einen „Beziehungsstatus" in ihrem Profil angegeben hatten (vgl. Backstrom et al 2013)

Soziale Netzwerke analysieren

Der Schwerpunkt lag auf der Analyse der Verbindungen der NutzerInnen untereinander. Um **romantische Beziehungen** zwischen zwei NutzerInnen zu erkennen, wurde nicht nur die Anzahl der gemeinsamen Kontakte untersucht, sondern auch, wie dicht diese gemeinsamen Kontakte untereinander vernetzt sind. Im Endeffekt konnte der eingesetzte Berechnungsalgorithmus in **60% der Fälle** unter den Kontakten den richtigen Partner bzw. die richtige Partnerin erkennen, wenn die Angabe des Beziehungsstatus im Profil als Vergleichsbasis verwendet wurde.

Der Algorithmus konnte sogar eingeschränkt prognostizieren, ob sich Paare in absehbarer Zeit trennen würden. Bei - durch die Angabe ihres Beziehungsstatus identifizierten - Paaren, die der Algorithmus nicht also potenzielle Paare erkannt hatte, wurde anhand der vorliegenden Daten **eine um 50% höhere Wahrscheinlichkeit einer Trennung** innerhalb von zwei Monaten verifiziert.

Viele ähnliche Arten persönlicher Daten

Dabei wird deutlich, welches Potenzial allein in der Analyse der sozialen Netzwerke zwischen Menschen steckt – unabhängig davon ob diese Verbindungsdaten in Form von *Facebook*-Kontakten oder in anderer Form vorliegen. Ähnliche Prognosen lassen sich aus der Analyse von Kontakten per **Telefon**, **SMS**, **E-Mail** oder auf jeglichen anderen Online-Plattformen, die **soziale**

44 Talbot, David (2012): A Phone that Knows Where You're Going. MIT Technology Review, 09.07.2012. Abgerufen am 14.09.2014 von http://www.technologyreview.com/news/428441/a-phone-that-knows-where-youre-going/

Netzwerkfunktionen bieten, treffen.

Facebook führt regelmäßig[45] **Experimente mit NutzerInnen** durch. Bei einer 2014 veröffentlichten und höchst umstrittenen Studie über Emotionen wurde das Verhalten von NutzerInnen nicht nur ohne deren Wissen untersucht, sondern es wurde dabei auch noch deren *News-Feed* manipuliert (vgl. Kramer 2014).

45 Hill, Kashmir (2014): 10 Other Facebook Experiments On Users, Rated On A Highly-Scientific WTF Scale. Forbes, 10.07.2014. Abgerufen am 14.09.2014 von http://www.forbes.com/sites/kashmirhill/2014/07/10/facebook-experiments-on-users/

3.3. Praktischer Einsatz in Marketing sowie Versicherungs-, Finanz- und Personalwirtschaft

„Daten-Wissenschafter haben Wege gefunden, vorherzusagen, wie Wähler wählen werden, wie Patienten eine Behandlung annehmen werden oder wie Kreditnehmer ihre Schulden zurückbezahlen werden. Es dauerte nicht lange, bis das Personalwesen entdeckt hat, dass die gleichen Technologien und Ansätze dazu eingesetzt werden können, um zu prognostizieren, wie sich Angestellte in Bezug auf Schlüssel-Metriken wie Fluktuation und Leistung verhalten werden"[46]

Greta Roberts, CEO der Personalwirtschaft-Beratungsfirma Talent Analytics, 2014

Facebook-Postings und Charakter

Insbesondere das zuvor beschriebene „Big Five"-Persönlichkeitsmodell zur Analyse von Charaktereigenschaften erfreut sich in vielen Bereichen großer Beliebtheit, nicht nur in der Wissenschaft. Auf der Website der ***Five Labs***[47] können sich etwa *Facebook*-NutzerInnen deren Charakterprofil aus einer Analyse der eigenen *Facebook*-Postings errechnen lassen. Dazu muss der *App* die Erlaubnis erteilt werden, auf deren *Facebook*-Postings zuzugreifen. Die *App* führt eine linguistische Analyse der Posting-Texte durch und basiert auf einer Studie der *University of Pennsylvania*, die wiederum auf einer Analyse von 700 Millionen Wörtern, Phrasen und Themen der *Facebook*-Postings von 75.000 TeilnehmerInnen beruht (vgl. Schwartz et al 2013)

Britischer Geheimdienst

Auch der britische Geheimdienst **GCHQ** beschäftigt sich mit dem Modell, wie aus einem der von Edward Snowden veröffentlichten Dokumente hervorgeht[48]. In der Präsentation wird eine Grafik gezeigt, die darstellt, wie Charaktereigenschaften mit den benutzten Web-Browsern wie *Chrome*, *Firefox*, *Safari* oder *Internet Explorer* korrelieren.

Twitter-Profile

IBM testet den Einsatz für Marketingzwecke und analysiert dazu öffentlich zugängliche Twitter-Profile[49]. Michelle Zhou, Leiterin der „User Systems and Experience Research Group" bei *IBM* erklärte dazu, dass extrovertierte Menschen mehr Bedürfnis nach Belohnungen und Aufmerksamkeit hätten – beispielsweise in der Form von „Punkten" in einem Flug-Bonusmeilenprogramm. In einem Callcenter könne abhängig vom Charakter unterschiedlich reagiert werden. Außerdem geht sie davon aus, dass sich durch die Berücksichtigung dieser Analysen die Konversionsraten[50] bei E-Mail- oder Telefon-Marketing verbessern würden.

Prognose der Kreditwürdigkeit

Die NutzerInnen werden allerdings üblicherweise nie nur auf ein einziges Kriterium hin untersucht, das „Big Five"-Modell ist nur einer von vielen möglichen Ansatzpunkten. Der Gründer von

---

46 Übersetzung durch den Verfasser, im Original: "Data scientists created the means to predict how voters will vote, or how patients will follow treatment protocols, or how borrowers will pay off debts. It wasn't long before HR realized the same technologies and approaches could be applied to predicting how employees will behave around key metrics like attrition and performance." Quelle: Roberts, Greta (2014): Making The Business Case For Predictive Talent Analytics. SAP Business Innovation, 12.05.2014. Abgerufen am 20.09.2014 von http://blogs.sap.com/innovation/human-resources/making-business-case-predictive-talent-analytics-01250921

47 http://labs.five.com (Abgerufen am 14.09.2014)

48 NBC News Investigations: GCHQ PowerPoint Slideshow Presentation 2012. Abgerufen am 14.09.2014 von http://msnbcmedia.msn.com/i/msnbc/Sections/NEWS/snowden_youtube_nbc_document.pdf

49 Simonite, Tom (2013): Ads Could Soon Know If You're an Introvert (on Twitter). MIT Technology Review, 08.11.2013. Abgerufen am 14.09.2013 von http://www.technologyreview.com/news/520671/ads-could-soon-know-if-youre-an-introvert-on-twitter/

50 Die sogenannte „Konversion" bezeichnet im Marketing die Umwandlung des Status einer Zielperson in einen neuen Status – beispielsweise die Umwandlung von InteressentInnen in KundInnen: http://de.wikipedia.org/wiki/Konversion_(Marketing)

zest finance[51] Douglas Merrill hat das beispielsweise so formuliert: „Alle Daten sind Kreditdaten, wir wissen nur noch nicht, wie wir sie richtig einsetzen". Das Unternehmen berechnet die Kreditwürdigkeit von Privatpersonen auf Basis von **70.000 verschiedenen Signalen**[52] aus unterschiedlichsten Quellen und wurde vom ehemaligen Leiter der Abteilung „Customer Segments" der US-Großbank *Capital One* und von Douglas Merrill - ehemaliger *Chief Information Officer* von *Google* - gegründet. Letzterer hat erklärt, das sei „die Mathematik, die wir bei Google gelernt haben." [53] Dort wäre für die Reihung der Suchergebnisse wichtig gewesen, was auf der jeweiligen Website stünde. Aber auch, wie gut die Grammatik sei, welche Schriftart eingesetzt würde und wann die Website erstellt oder geändert worden sei. „Daten sind wichtig. Mehr Daten sind immer besser."

Einbeziehung von Social Media

Das Hamburger Unternehmen ***Kreditech***[54] nutzt für die Prognose der Bonität unter anderem Standort-Informationen und verlangt von den Betroffenen Zugriff auf deren Profile auf *Facebook*, *Xing* oder *LinkedIn* – die Ebay-Profile wären ohnehin öffentlich zugänglich[55]. Bei der Berechnung der Bonitätseinschätzungen würden über **15.000 Datenpunkte** einfließen: Beim Online-Kreditantrag würde nicht nur berücksichtigt, welches Gerät die NutzerInnen verwenden und welche *Apps* sie installiert haben, sondern auch die Zeit, die sie für das Ausfüllen des Formulars benötigen – oder die Häufigkeit der Nutzung der Löschtaste. *Kreditech* ist in 12 Ländern von Spanien, Polen, Russland, Brasilien bis Australien tätig und vergibt kurzfristige Kredite bis zu einem Betrag von € 500. In Deutschland wurde der Geldverleih nach drei Wochen wieder eingestellt.

Mobilfunk-Metadaten

Das US-Unternehmen ***Cignifi*** [56]hingegen nutzt genau die einige Kapitel zuvor beschriebenen Mobilfunk-Metadaten zur Prognose der Kreditwürdigkeit. Basis für die Bewertungen sind laut Eigenangabe ausschließlich 4 Wochen Anruf-Metadaten, das Vorliegen einer Zahlungshistorie sei nicht notwendig. *Cignifi* bietet mehrere unterschiedliche Score-Varianten an: Weitere Produkte wie *Cignifi Response*[57] messen die Wahrscheinlichkeit, dass KonsumentInnen auf bestimmte Angebote reagieren – etwa auf Mailings, Telemarketing, E-Mail oder SMS.

Prognose von Gesundheits-risiken

Aviva[58] – die fünftgrößte Versicherungsgesellschaft der Welt – hat laut *Wall Street Journal* mit einem von der Beratungsfirma *Deloitte* entwickelten Vorhersagemodell untersucht, ob sich deren traditionellen Verfahren zur Gesundheitsuntersuchung auf Basis von Blut- und Urinproben durch eine Prognose aus Marketingdaten zum Konsumverhalten ersetzen lassen könnten (vgl. Scism 2010). Für den Test wurden für 60.000 bestehende KundInnen Daten gekauft – etwa über Konsumverhalten, Lebensstil oder Einkommen. Ziel war es, daraus die Risiken für Krankheiten wie Diabetes, hohen Blutdruck oder Depression abzuschätzen. Laut John Currier – Versicherungsmathematiker bei *Aviva* – waren die Ergebnisse nahe an den traditionellen Verfahren der Gesundheitsuntersuchung.

---

51 http://www.zestfinance.com

52 Crosman, Penny (2013): ZestFinance Aims to Fix Underwriting for the Underbanked. American Banker, 29.11.2013. Abgerufen am 14.09.2014 von http://www.americanbanker.com/issues/177_223/zestfinance-aims-to-fix-underwriting-for-the-underbanked-1054464-1.html

53 Hardy, Quentin (2012): Just the Facts. Yes, All of Them. New York Times, 25.03.2012. Abgerufen am 14.09.2014 von http://www.nytimes.com/2012/03/25/business/factuals-gil-elbaz-wants-to-gather-the-data-universe.html

54 http://www.kreditech.com

55 Schulz, Thomas; Müller, Martin; Rosenbach, Marcel (2013): Die Daten-Bank. Spiegel, 14.05.2013. Abgerufen am 14.09.2014 von http://www.spiegel.de/netzwelt/netzpolitik/big-data-daten-bank-a-899538.html

56 http://www.cignifi.com (Abgerufen am 14.09.2014)

57 http://www.cignifi.com/en-us/technology (Abgerufen am 14.09.2014)

58 http://de.wikipedia.org/wiki/Aviva

Personal-wirtschaft

Auch viele Personalabteilungen großer Unternehmen haben inzwischen eigene Analytics-Abteilungen eingerichtet. Die *Big Five* werden schon bisher als einer von mehreren Eignungstests in Personalauswahl und -psychologie eingesetzt[59]. Der Öl-Gigant *Royal Dutch Shell* setzt das Produkt ***Knack*** [60] ein, das mittels eines Videospiels das Potenzial von BewerberInnen und Angestellten bewertet. Dabei wird jede einzelne Spiel-Interaktion detailliert aufgezeichnet und ausgewertet – etwa wie lange die ProbandInnen vor bestimmten Aktionen zögern, oder wie sie Probleme lösen[61]. Die Rohdaten aus dem Spiel werden mit anderen Daten abgeglichen und darin nach Mustern gesucht. Schlussendlich werden Bewertungen über das kreative Potenzial, Durchhaltevermögen, Lernkapazität, soziale Intelligenz, Charakter oder über die Fähigkeit, aus Fehlern zu lernen, berechnet.

Drei Millionen BewerberInnen und Angestellte…

Die Firma ***Evolv***[62] bezeichnet sich als „leader in big data workforce optimization" und hat nach eigener Angabe Zugriff auf umfassende Daten von über drei Millionen BewerberInnen und Angestellten – mit unterschiedlichen Job-Profilen und aus Unternehmen aus unterschiedlichen Wirtschaftssektoren[63]. Die über 500 Millionen[64] gesammelten Datenpunkte stammen aus ausführlichen Fragebögen, die von den Angestellten und BewerberInnen ausgefüllt wurden, umfassen aber auch deren Beschäftigungshistorie oder Daten über deren Arbeitsleistung – etwa in Form von Rückmeldungen über die Kundenzufriedenheit. *Evolv* beschäftigt sich damit, Zusammenhänge und Muster in diesen Daten zu finden und damit ihren Unternehmenskunden dabei zu helfen, BewerberInnen und Angestellte zu bewerten. In die Bewertung einbezogen wurden bereits Aspekte wie die Anzahl der „Social Media"-Accounts oder dem benutzten Browser bei der Online-Bewerbung[65].

Daten über Angestellte zusammenführen

Die in der Personalwirtschaft eingesetzten Überwachungs- und Analyse-Methoden werden oft unter dem euphemistischen Begriff **Talentmanagement**[66] gefasst und betonen meist die Herausforderungen in Bezug auf Personalgewinnung und –bindung. In einem von ***Oracle*** - einem der international größten Anbieter von Unternehmens-Software – veröffentlichten Report über „Talentanalyse und Big Data" wird das „Problem" angesprochen, dass Unternehmen die Daten über ihre Angestellten in voneinander getrennten „Silos" verwalten würden (vgl. CIPT/Oracle 2013). Daten über Demographie, Fähigkeiten, Anwesenheit, Teilnahme an Schulungen und Projekten oder über deren Leistung sollten über Unternehmensbereiche und Projekte hinweg „geteilt" und dazu genutzt werden, „sinnvolle" Erkenntnisse zu gewinnen und damit bessere „Entscheidungen" treffen zu können. Das US-Startup ***ConnectCubed***[67] bietet beispielsweise genau das an: Die Vorhersage der zukünftigen Leistung von Angestellten anhand von von Unternehmen zur Verfügung gestellten Daten (z.B. „Performance reviews, date and source of hire, job

59 Sarges W., Wottawa H. (Hrsg.) (2004): Handbuch wirtschaftspsychologischer Testverfahren, Band I: Personalpsychologische Instrumente (2. Auflage). Papst Science Publishers, Lengerich.

60 https://www.knack.it

61 Peck, Don (2013): They're Watching You at Work. What happens when Big Data meets human resources? The emerging practice of "people analytics" is already transforming how employers hire, fire, and promote. The Atlantic, 20.11.2013. Abgerufen am 19.09.2014 von http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/

62 http://www.evolv.net (Abgerufen am 14.09.2014)

63 Javers, Eamon (2014): Inside the wacky world of weird data: What's getting crunched. CNBC, 12.02.2014. Abgerufen am 14.09.2014 von http://www.cnbc.com/id/101410448

64 Evolv (2013): Evolv achieves Triple Digit Booking Growth for its big data workforce solutions. Press Release. Abgerufen am 14.09.2014 von http://www.evolv.net/company/news-and-events/press-releases/evolv-achieves-triple-digit-booking-growth-big-data-workforce-solutions/

65 Ito, Aki (2013): Hiring in the Age of Big Data. Bloomberg Businessweek, 24.10.2013. Abgerufen am 14.09.2014 von http://www.businessweek.com/articles/2013-10-24/new-way-to-assess-job-applicants-online-games-and-quizzes

66 http://de.wikipedia.org/wiki/Talentmanagement

67 http://connectcubed.com (Abgerufen am 20.09.2014)

family descriptions, interview scores, personality, aptitude, and skill test results"[68]).

Gezielt werben in emotionalen Momenten

Am weitesten fortgeschritten sind derartige Analyse-Technologien aber im reinen **Online-Bereich**. Das US-Werbeunternehmen ***MediaBrix*** hat ein System entwickelt[69], das in Echtzeit die Emotionen von ComputerspielerInnen analysiert und in besonders geeigneten Momenten personalisierte „immersive"[70] Werbung und „dynamisch positionierte, kreative" Angebote platziert. Mit dieser von *MediaBrix* als „Emotional Targeting" bezeichneten Technologie könnten Werbetreibende die SpielerInnen gezielt während sogenannter „Breakthrough Moments" ansprechen - und eine große Bandbreite von Emotionen zwischen „Begeisterung und Frustration" erkennen. *MediaBrix* erreicht in den USA über 45 Millionen monatliche NutzerInnen und damit 46% des gesamten Publikums im Bereich Online Gaming. Durch den Einsatz von „Emotional Targeting" wäre die „Performance" im Web um 15% und bei mobilen *Apps* um 30% gestiegen.

Microsoft hat 2012 ein Patent auf „Targeting Advertisments Based on Emotion" angemeldet[71], ***Samsung*** hat 2013 das Patent „Apparatus and method for sharing user's emotion" angemeldet[72], das in eine ähnliche Richtung geht.

3.4. Personalisierte Preisdiskriminierung im Online-Handel?

Dynamische Preisgestaltung[73] bzw. Preisdifferenzierung[74] ist in Bereichen wie Reisen (z.B. Flüge, Hotels), Unterhaltung (z.B. Tickets für Veranstaltungen) und Einzelhandel (z.B. Lebensmittel) schon lange üblich. Dabei variieren die Preise je nach Kauf- oder Buchungszeitpunkt - und abhängig vom Lagerstand, verfügbaren Plätzen, der Beliebtheit des Produkts, des gebuchten Zeitpunkts - oder abhängig von den Preisen der Konkurrenz. Auch die Einbeziehung von individuellen Eigenschaften in die Preisgestaltung ist manchmal üblich (z.B. Rabatte für Kinder, Jugend, Familien oder SeniorInnen). Neu ist aber die Einbeziehung digitaler persönlicher Daten und Verhaltensweisen in mehr oder weniger komplexe statistische Prognosemodelle, um die Preise in Echtzeit zu individualisieren.

Preis- und Suchdiskriminierung

Jakub Mikians et al (2012) unterscheiden zwischen Preisdiskriminierung und Suchdiskrimierung. **Preisdiskriminierung** wird als eine Praxis definiert, bei der das gleiche Produkt für unterschiedliche KäuferInnen zu unterschiedlichen Preisen angeboten wird – abhängig von einem angenommen Maximalpreis, den die jeweiligen KäuferInnen zu zahlen bereit sein könnten. Preisdiskriminierung wird klar abgegrenzt von einer Art von Preisdifferenzierung, bei der etwa unterschiedliche Filialen einer Handelskette das gleiche Produkt zu unterschiedlichen Preisen anbieten, um den Lagerstand in einer Filiale zu reduzieren - oder weil eine Filiale einen billigeren Lieferanten hat. **Suchdiskriminierung** wird hingegen als Praxis gefasst, bei der etwa in einer bestimmten Produktkategorie für manche NutzerInnen teurere Produkte angeboten werden. Da die wenigsten NutzerInnen mehr als die erste Seite der Suchergebnisse ansehen, würden sie dadurch in einen bestimmten Preis-Bereich „gelenkt".

---

68 http://connectcubed.com/benchmark (Abgerufen am 20.09.2014)

69 MediaBrix (2013): The MediaBrix Social and Mobile Gaming Report. Q3-4 2013. Abgerufen am 20.09.2014 von http://www.mediabrix.com/wp-content/uploads/2014/03/MediaBrix_Report_Q3-4_2013_FINAL.pdf

70 http://de.wikipedia.org/wiki/Immersion_(virtuelle_Realit%C3%A4t)

71 Microsoft Corporation (2012): Targeting Advertisements Based on Emotion, US 20120143693 A1. Abgerufen am 14.09.2014 von http://www.google.com/patents/US20120143693

72 Samsung Electronics Co., Ltd. (2013): Apparatus and method for sharing user's emotion. US 20130144937 A1. Abgerufen am 14.09.2013 von http://www.google.com/patents/US20130144937

73 http://de.wikipedia.org/wiki/Dynamic_Pricing

74 http://de.wikipedia.org/wiki/Preisdifferenzierung

Teurere Angebote bei Mac-Nutzung

Das börsennotierte Online-Reisebuchungsportal ***Orbitz***[75] hat beispielsweise 2012 bestätigt, dass sie „Experimente" durchgeführt hätten, bei denen *Mac*-NutzerInnen eine Auswahl teurerer Hotels angeboten wurde als *PC*-NutzerInnen, da man herausgefunden habe, dass Mac-NutzerInnen im Durchschnitt 20 bis 30 Dollar mehr für eine Hotelnacht ausgeben als PC-NutzerInnen. Ein Test des *Wall Street Journal* (vgl. Mattioli 2012) hat belegt, dass bei einer Suche nach einem Hotel in Miami Beach für zwei bestimmte Nächte auf der ersten Ergebnisseite bei Nutzung eines Mac-Computers andere und um **durchschnittlich 11% teurere Resultate** angezeigt wurden als bei Nutzung eines PC. Bei einem anderen Ort betrug der Unterschied sogar 13%. Ein Sprecher von *Orbitz* hat bestätigt, dass auch Faktoren wie der Standort der NutzerInnen, deren vergangenes Verhalten auf der Website oder die Art der Website, von der aus sie auf das Angebot gekommen sind, einen Einfluss auf die angezeigten Ergebnisse habe.

Standort und Online-Verhalten

In weiteren systematischen Tests des *Wall Street Journal* (vgl. Valentino-Devries et al 2012) konnte festgestellt werden, dass der große US-Bürobedarfshändler ***Staples***[76] abhängig vom Standort unterschiedliche Preise im Online-Shop anbietet. Im Rahmen der Tests wurde entdeckt, dass die Website die Postleitzahl der BesucherInnen in einem Browser-Cookie speichert. Durch gezielte Manipulation dieser Postleitzahl wurden Tausende Besuche mit unterschiedlichen Postleitzahlen im Online-Shop von *Staples* simuliert und dabei die angebotenen Preise verglichen. Bei einem Test mit 29.000 Postleitzahlen und 1.000 zufällig ausgewählten Produkten wurde eine **durchschnittliche Preisdifferenz von 8%** festgestellt. Auch bei anderen Unternehmen wie *Discover Financial Services*, *Rosetta Stone* oder *Home Depot* wurde festgestellt, dass abhängig von verschiedenen Charakteristika der NutzerInnen unterschiedliche Preise angeboten wurden. Der US-Bürobedarfshändler *Office Depot* hat in der Folge bestätigt, dass **Standort und Website-Nutzungsverhalten** die Auswahl der im Online-Shop angebotenen Produkte beeinflussen würden. Auch bei der US-Baumarktkette *Home Depot* war der Preis vom Standort der Shop-NutzerInnen abhängig. Die Firma bestätigt, für die Einschätzung des Standorts die IP-Adressen der NutzerInnen zu verwenden.

Personalisierte Rabatte

Das von einem ehemaligen *Facebook*-Produktmanager gegründete Unternehmen ***Freshplum***[77] bietet ein Service für den Online-Handel, das individuelle Preis-Rabatte für einzelne KundInnen berechnet, um die Verkäufe zu steigern. Dabei wird versucht, NutzerInnen zu identifizieren, die ohne Preis-Rabatt keinen Kauf tätigen würden. In die Analyse einbezogen werden laut Eigenangabe Informationen wie der aktuelle Standort der NutzerInnen (z.B. „Stadtzentrum oder Vorort") oder das Wetter an diesem Standort (vgl. Tanner 2014). *Freshplum* wird unter anderem von Online-Handelsunternehmen in den Bereichen Kosmetik oder Luxusgüter eingesetzt, seit 2011 ist *Google* an der Firma beteiligt.

Schwer zu entlarven

Eine spanische Studie (vgl. Mikians et al 2012) hat in einem aufwändigen Forschungsdesign 600 Produkte in 35 Produktkategorien auf **200 großen internationalen Online-Shops** untersucht und dabei ebenfalls individualisierte Preisgestaltung bzw. eine individuell andere Auswahl von billigeren oder teureren Produkten in den Suchergebnissen beobachtet. Starke Indizien sprechen dafür, dass die festgestellten Unterschiede bei Preisen und den angebotenen Produkten von **bis zu 166%** teils auf dem Standort der NutzerInnen basieren - aber auch auf deren vermuteter finanzieller Situation sowie der Website, über die sie auf den jeweiligen Online-Shop gekommen sind. Für die Analyse des Einflusses der finanziellen Situation auf die Preise wurden NutzerInnen simuliert, die sich zuvor sieben Tage in einer bestimmten Art und Weise automatisiert und systematisch auf einer Auswahl von 100 populären Websites bewegt haben und dabei

75 http://en.wikipedia.org/wiki/Orbitz
76 http://de.wikipedia.org/wiki/Staples
77 https://www.freshplum.com (Abgerufen am 20.09.2014)

viele Daten hinterlassen haben – auch durch die auf den Websites eingebundenen externen Tracking-Services.

KonsumentInnen haben keine Chance

Hier zeigt sich die Komplexität derartiger Untersuchungen. Es ist weder bekannt, welche individuellen Variablen die Online-Shops mit welchen Algorithmen in die Preisgestaltung einbeziehen, noch ist bekannt, welche persönlichen Daten überhaupt genutzt werden, inwieweit NutzerInnen identifiziert werden können oder ob Daten zugekauft werden. KonsumentInnen haben bei derartigen Praktiken keinerlei Chance mehr, zu verstehen, ob und wie ihr individueller Preis oder die Auswahl der ihnen angebotenen Produkte zustande kommen. Die Situation verschlimmert sich, wenn in Zukunft noch avanciertere Prognosemethoden auf Basis von umfangreichen Informationen über das Verhalten der NutzerInnen und von statistischer Korrelationen zum Einsatz kommen.

3.5. Identifikation und De-Anonymisierung von NutzerInnen

Anonymisierte oder pseudonymisierte Datensätze werden beispielsweise bei wissenschaftlicher Forschung eingesetzt, spielen aber generell bei digitaler Kommunikationstechnologie in vielen Bereichen eine große Rolle – nicht zuletzt in Hinblick auf Datenschutz. Bei der **Anonymisierung** persönlicher Datensätze soll jeglicher Bezug auf konkrete, einzelne Personen aus diesen Datensätzen entfernt und damit eine Identifikation einzelner Personen unmöglich gemacht werden. Bei der **Pseudonymisierung** werden Namen oder andere Identifikationsmerkmale durch Pseudonyme oder Codes ersetzt (z.B. Buchstaben- oder Zahlenkombinationen). Dabei können sich einzelne Datensätze weiterhin aufeinander beziehen und beispielsweise einzelne Telefonate oder Suchanfragen weiterhin einer bestimmten Person zugeordnet werden, ohne dass diese Person identifiziert werden kann (vgl. Pfitzmann et al 2010). Die Pseudonymisierung kann allerdings rückgängig gemacht werden, wenn der Schlüssel bekannt ist – also wenn an anderer Stelle die Zuordnung von Namen zu Pseudonymen vorliegt.

Einzigartige Kombinationen von Eigenschaften

Je nach Art und Umfang der anonymisierten oder pseudonymisierten Datensätze können Personen trotzdem identifiziert werden. Wenn ein Datensatz etwa keine Namen enthält, aber **Initialen und Geburtsdaten**, kann die Person in vielen Fällen mit Hilfe von anderen Datenbanken oder teils öffentlich zugänglichen Informationen bestimmt werden, da die Kombination aus Initialen und Geburtsdatum in vielen Fällen relativ einzigartig ist[78]. Eine Untersuchung aus 1990 hat gezeigt, dass die Kombination aus **Postleitzahl, Geschlecht und Geburtsdatum** bei 216 von 248 Millionen und damit 87% der US-AmerikanerInnen einzigartig ist und damit eine Identifikation ermöglicht (vgl. Sweeney 2002). Datensätze, die derartige Angaben enthalten, können nicht als anonymisiert betrachtet werden. Die Entfernung von relativ offensichtlichen Attributen wie Namen, Sozialversicherungsnummern oder IP-Adressen reicht bei weitem nicht aus.

„Anonyme" Suchanfragen

Je ausführlicher eine Datensammlung ist, je mehr ergänzende Informationen aus anderen Quellen zur Verfügung stehen und je weiter fortgeschrittene Technologien eingesetzt werden, desto eher ist die Identifikation von Personen auch dann möglich, wenn Datensätze scheinbar anonymisiert sind. Diese Problematik hat sich massiv verstärkt, seit immer umfassendere digitale Datenmengen über Personen gespeichert und verarbeitet werden. 2006 hat beispielsweise *AOL* detaillierte Log-Dateien zum **Suchverhalten** von 675.000 Personen veröffentlicht, einzelne Nut-

78 Pelleter, Jörg (2011): Organisatorische und institutionelle Herausforderungen bei der Implementierung von Integrierten Versorgungskonzepten am Beispiel der Telemedizin. Schriften zur Gesundheitsökonomie, Universität Erlangen Lehrstuhl für Gesundheitsmanagement, S. 296ff

zerInnen konnten allein aus einer Analyse der Suchanfragen identifiziert werden.[79]

„Anonyme" Film-bewertungen

In den letzten Jahren sind statistische De-Anonymisierungsmethoden entwickelt worden: Eine US-Studie hat demonstriert, dass einzelne Datensätze in einer Datenbank mit **Filmbewertungen** von 500.000 AbonnentInnen des Online-Diensts *Netflix* leicht konkreten Personen zugeordnet werden konnten, wenn etwas Hintergrundwissen über diese Personen vorhanden ist (vgl. Narayanan et al 2008). Dazu wurden die *Netflix*-Filmbewertungen mit öffentlich zugänglichen Rezensionen auf der Website *imdb.com* verknüpft, auf denen die NutzerInnen oft unter Echtnamen veröffentlichen. Für die Identifikation waren im Schnitt 2-8 Filmbewertungen pro NutzerIn ausreichend und es war kein Problem, wenn die Daten der Filmrezensionen etwas fehlerhaft waren.

Daten von Mobilfunk-Unternehmen

Eine 2013 im Magazin *Nature* veröffentlichte Studie hat die Daten von 1,5 Millionen **Mobiltelefon-NutzerInnen** analysiert und belegt, dass vier aus Aufenthaltsort und Zeitpunkt bestehende Datenpunkte genügen, um 95% der NutzerInnen eindeutig zu identifizieren (vgl. Montjoye et al 2013). Diese Kombination aus vier Aufenthaltsorten und den entsprechenden Zeitpunkten ist bei unterschiedlichen Personen hochgradig einzigartig. Es ist davon auszugehen, dass sich auch bei anderen Klassen persönlicher Daten wie bei **Einkäufen**, **Empfehlungen**, ***Likes***, **Suchbegriffen** oder **aufgerufenen Websites** ähnliche Ergebnisse erzielen lassen würden.

Wiedererkennung von NutzerInnen

Unter Begriffen wie „Browser Fingerprint" oder **Device Fingerprint**[80] wird seit einigen Jahren die eindeutige Wiedererkennung von NutzerInnen anhand der Eigenschaften des benutzten Web-Browsers und Geräts diskutiert – ohne dass dabei *Cookies*[81] auf den Rechnern der NutzerInnen gespeichert werden müssen. Einige Daten der NutzerInnen werden bei jedem Klick an die AnbieterInnen gesendet – beispielsweise Angaben über das benutzte Betriebssystem, dessen Version und die installierten Schriftarten – oder über den benutzten Web-Browser, den installierten Erweiterungen und deren genaue Versionsnummern. Wie mehrere Untersuchungen belegt haben, ist die Kombination dieser Eigenschaften hochgradig individuell und eindeutig (vgl. Nikiforakis 2013). Ein Forschungsprojekt[82] der US-Bürgerrechtsorganisation *Electronic Frontier Foundation* (EFF) hat ergeben, dass 99,1% der untersuchten Browser-NutzerInnen auf Basis ihres *Browser Fingerprints* korrekt wiedererkannt werden konnten – bei einer Fehlerrate von nur 0,86% (vgl. Eckersley 2010).

Darüber hinaus können auch **biometrische Daten** aus Iris-, Stimm- oder Gesichtserkennung oder aus Analysen von Bewegungsmustern, Mausnutzung, Tippdynamiken (vgl. Mudholkar 2012) und viele mehr zur digitalen Wiedererkennung einzelner Personen genutzt werden - genauso wie traditionelle Fingerabdrücke oder DNA-Profile.

---

79 Barbaro, M.; Zeller, T. (2006): A Face Is Exposed for AOL Searcher No. 4417749. New York Times, 09.08.2006. Abgerufen am 27.09.2014 von http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all

80 http://en.wikipedia.org/wiki/Device_fingerprint

81 http://de.wikipedia.org/wiki/Cookie

82 An der Untersuchung kann weiterhin teilgenommen werden: https://panopticlick.eff.org (Abgerufen am 27.09.2014)

4 Datenhungrige Geräte und Plattformen

„Er hatte den Sieg über sich selbst errungen. Er liebte den großen Bruder“[83]
Letzter Satz im Roman „1984“ von George Orwell, 1949

Smartphones und die darauf installierten ***Apps*** sind eines der größten „Einfallstore“ für Unternehmen, die persönliche Daten über NutzerInnen sammeln. Die von **Fitness-Trackern**, ***Smartwatches*** und entsprechenden *Apps* gemessenen Daten über den eigenen Körper und die Gesundheit haben großes kommerzielles Potenzial. **Auto-Versicherungstarife** auf Basis von Rundum-Überwachung könnten zum Vorbild für andere Bereiche werden. Im ***Internet der Dinge*** wird die Überwachung durch vernetzte Sensoren omnipräsent. Im folgenden Kapitel sollen diese vier Felder näher untersucht werden.

4.1. Smartphones und Apps: Spione in der Hosentasche

Mobile Kommunikationstechnologie hat sich rasant verändert in den letzten 25 Jahren. Ende der 1980er Jahre brachte kaum ein Mobiltelefon weniger als ein Kilogramm auf die Waage und konnte nur für einen Zweck verwendet werden: Telefonanrufe. Seit der Einführung des ersten *Apple iPhone* im Jahr 2007 haben nun *Smartphones* herkömmliche Mobiltelefone über weite Strecken abgelöst. Laut IDC[84] wurden global 2013 erstmals über **eine Milliarde** Einheiten verkauft, nach etwa 700 Millionen Einheiten 2012. Die Studie „Aktuelle Fragen der Geodaten-Nutzung auf mobilen Geräten“ des österreichischen *Instituts für Technikfolgenabschätzung* hat sich umfassend mit *Smartphones* und der Analyse und kommerziellen Verwertung der damit erfassten Daten befasst (Rothmann et al 2012).

Funkverbindungen und Sensoren

Smartphones besitzen meistens mehrere Funkanbindungen zur Datenübertragung – von *WLAN* über *GSM*, *UMTS*, *HSPA/3G*, *LTE/4G* bis *Bluetooth* und *NFC* (vgl. Rothmann et al 2012). Außerdem weisen *Smartphones* eine Vielzahl an Sensoren auf - wie etwa Mikrofon, Kamera, GPS-Empfänger, Bewegungs-, Lage-, Licht-, Näherungs- und Magnetfeldsensoren. Neuere Modelle haben teils auch Barometer, Temperatur-, Luftfeuchtigkeits- oder Fingerabdrucksensoren integriert. Der Markt wird von den zwei Plattformen ***Android*** (Marktanteil 2013 laut IDC 78,6%) und ***iOS*** (15,2%) dominiert, andere Plattformen wie *Windows Phone* oder *Blackberry* führen inzwischen ein Nischendasein. Während das Betriebssystem *iOS* ausschließlich auf Geräten von *Apple* verwendet wird, kommt das von der von *Google* geführten „Open Handset Alliance“ entwickelte *Android* als Betriebssystem und Software-Plattform auf Geräten vieler Hersteller zum Einsatz.

Apps und deren Berechtigungen

Die Geräte beider Hersteller liefern eine Software-Grundausstattung aus, die grundlegende Funktionen wie Telefonie, Kontaktverwaltung, Kurznachrichten (SMS), Fotografie, Video und einige weitere Anwendungen abdeckt. Zusätzlich kann aber von Drittanbietern entwickelte Software installiert werden, die als ***Apps*** bezeichnet werden. *Apps* von Drittanbietern bieten den *Smartphone*-NutzerInnen vielfältige Anwendungsmöglichkeiten, mit April 2013 waren auf den beiden Plattformen *Android* und *iOS* jeweils über 800.000 *Apps* verfügbar[85]. Auf welche verfügbaren Sensoren und auf welche auf dem Gerät gespeicherten Daten eine *App* zugreifen kann, wird durch ein System aus **Berechtigungen** bestimmt. Bei *Android* werden die angeforderten

83 Orwell, George. 1984. Ein utopischer Roman. Diana, Zürich.
84 http://www.idc.com/getdoc.jsp?containerId=prUS24645514 (Abgerufen am 06.07.2014)
85 McCracken, H. (2013): Who’s Winning, iOS or Android? All the Numbers, All in One Place., Time Magazine, 16.04.2013 http://techland.time.com/2013/04/16/ios-vs-android (Abgerufen am 07.07.2014)

Berechtigungen - beispielsweise Zugriff auf die Kontaktliste oder die Standort-Daten - vor Installation einer *App* in Form einer Liste angezeigt. Ohne Zustimmung zu allen angeforderten Berechtigungen kann eine *App* nicht installiert werden. Bei *iOS* besitzt jede installierte *App* bestimmte Standard-Berechtigungen (z.B. Zugriff auf das Internet), für andere Berechtigungen (z.B. Standort, Kontakte, Mikrofon oder Bewegungssensor) fragt *iOS* erst dann beim NutzerInnen nach, sobald eine *App* auf diese Ressourcen zugreifen möchte.

Spione in der Hosentasche?

Ein *Smartphone* wird meist von einer einzelnen Person verwendet, von dieser permanent bei sich getragen und gilt daher als sehr persönliches und privates Gerät, das ungern an Unbekannte weitergegeben wird (vgl. Urban et al 2012). Allein die elementaren auf dem Gerät gespeicherten Daten wie Anrufe, Kurznachrichten, Kontaktlisten, Kalender, Fotos, Videos, besuchte Webseiten oder Standort-Daten bzw. Bewegungsverhalten ermöglichen weitgehende **Einblicke in Persönlichkeit und Alltag** der BesitzerInnen. Auf dem Gerät sind nicht nur Informationen zu FreundInnen und Familie gespeichert, sondern etwa auch Kontakte in den Lebensbereichen Arbeit, Finanzen oder Gesundheit. Die Geräte sind meist durchgängig mit dem Internet verbunden, die integrierten Sensoren können potenziell immer aktiv sein. Auf einem *Smartphone* sind oft viele Passwörter gespeichert, die Zugang zu den persönlichen BenutzerInnen-Accounts von E-Mail über soziale Netzwerke bis E-Commerce ermöglichen. Risiken für die Privatsphäre der NutzerInnen ergeben sich potenziell in mehrerer Hinsicht:

Risiken für die Privatsphäre

- **Datensicherheit:** Unberechtigter Zugriff auf das Gerät (z.B. Verlust, Diebstahl) oder Sicherheitslücken in Betriebssystem und *Apps*, die von Computerviren, Trojanern oder durch gezielte individuelle Angriffe ausgenutzt werden[86].
- **Datenübertragung an App-Anbieter:** Speicherung, Verarbeitung und Weitergabe von persönlichen Daten durch *Apps* von Drittanbietern, die je nach angeforderten Berechtigungen auf verfügbare Sensor-Daten und andere auf dem Gerät gespeicherten Informationen zugreifen können und diese teils an weitere Unternehmen übertragen.
- **Datenübertragung an Plattform- bzw. *App-Store*-Betreiber:** Die meisten NutzerInnen von *Android* verknüpfen ihr Gerät mit einem *Google*-Account[87], laut *Google* wurden bis Mai 2013 insgesamt 900 Millionen[88] *Android*-Geräte bei *Google* aktiviert. Die meisten NutzerInnen von *iOS* verknüpfen ihr Gerät mit einem *Apple*-Account („Apple ID"[89]), da sich die Geräte ansonsten nicht sinnvoll einsetzen lassen.
- **Mobilfunk-Unternehmen:** Darüber hinaus werden auch von Mobilfunk-NetzbetreiberInnen Daten über die NutzerInnen gespeichert.

4.1.1. Datenmissbrauch durch Apps

Apps decken die unterschiedlichsten Lebensbereiche ab und sind oft zwingend auf die Zugriffsmöglichkeit auf bestimmte Daten angewiesen, damit sie ihre Funktion erfüllen können. Eine Kamera-*App* muss etwa zwingend auf die im Gerät verbaute Kamera zugreifen können, eine Routenplaner-*App* auf die Ortungs- und Standort-Daten, eine Adressbuch-*App* auf die gespeicherten

86 Heider, Jens and Khayari, Rachid El (2012): Geht Ihr Smartphone fremd? Datenschutz und Datensicherheit, 36/3/2012, S. 155-60. Abgerufen am 07.07.2014 von https://www.sit.fraunhofer.de/fileadmin/dokumente/artikel/DuD-Artikel_geht_ihr_Smartphone_fremd.pdf

87 http://en.wikipedia.org/wiki/Google_Account

88 Welch, C (2013): Google: 900 million Android activations to date, 48 billion app installs, The Verge, 15.05.2013 http://www.theverge.com/2013/5/15/4333584/total-android-activations-900-million (abgerufen am 07.07.2014)

89 http://en.wikipedia.org/wiki/Apple_ID (abgerufen am 07.07.2014)

Kontakte. Viele *Apps* fordern von den NutzerInnen allerdings Zugriffsberechtigungen auf Daten an, die für die eigentliche Funktion der Anwendung **nicht erforderlich** sind - oder übertragen Daten an **dritte Parteien**, ohne dass die NutzerInnen dieser Übertragung zugestimmt haben (vgl. Rothmann et al 2012).

Übertragung von Standort-Daten und Geräte-ID an Werbenetzwerke

Eine viel rezipierte Untersuchung des *Wall Street Journal* von *Android*- und *iOS-Apps* hat 2010 gezeigt, dass insgesamt **47 von 100 der populärsten *Apps* Standort-Daten** übertragen haben - die meisten davon nicht nur an die *App*-Anbieter, sondern auch an weitere Unternehmen (vgl. Thurm et al 2010). 56 davon haben die weltweit eindeutige ID der Geräte ohne Zustimmung der NutzerInnen an Dritt-Unternehmen übertragen – meistens an **Werbenetzwerke**. Vor allem die Entwickler kostenloser *Apps* integrieren oft Tracking-Module, die die übermittelten Daten etwa für die Einblendung von zielgruppenorientierter Werbung nutzen - aber manchmal auch anderweitig verwerten.

Die Musik-*App Pandora* übermittelte etwa zum Zeitpunkt der Untersuchung Alter, Geschlecht, Standort-Daten und Geräte-ID an mehrere Werbenetzwerke, die populäre Spiele-*App Angry Birds* unter anderem Adressbuch, Standort-Daten und Geräte-ID an ein externes Unternehmen. Die Dating-*App Grindr* sendete Geschlecht, Standort-Daten und Geräte-ID an drei Werbenetzwerke, die Spiele-*App PaperToss* Standort-Daten und Geräte-ID an fünf Werbenetzwerke, die Textnachrichten-*App textPlus* die Geräte-ID gleich an acht Werbenetzwerke.

Ortung im 30-Sekunden-Takt

Laut einer anderen US-Studie aus dem Jahr 2010 übermittelten **15 von 30 untersuchten *Android-Apps* Standort-Daten zu Werbenetzwerken** – und ohne die NutzerInnen darüber zu informieren (vgl. Enck et al 2010). In manchen Fällen wurden diese Standort-Informationen alle 30 Sekunden übertragen, in einem Fall sogar gleich nach der Installation – vor dem ersten Start der *App*. Eine weitere Untersuchung[90] von 94 *iOS-Apps* ergab 2011, dass **84% der analysierten Apps mit externen Domains Kontakt** aufnahmen und 74% zumindest die Geräte-ID an eine externe Domain übertragen haben.

Tools mit Nebenwirkungen

Laut einer Analyse der Zeitschrift c't aus 2012[91] übermittelten viele der **60 untersuchten *Apps* Daten an Werbenetzwerke** - die zu diesem Zeitpunkt beliebteste Taschenlampen-*App Flashlight* gleich an fünf davon. Der darin erwähnte Anbieter *Onavo* betreibt etwa ein Online-Service, das verspricht, durch Zwischenschaltung eines Proxy-Servers und Datenkompression für die NutzerInnen die teure mobile Datenübertragung zu reduzieren. Gleichzeitig übermittelten die *Apps* von *Onavo* laut c't unter anderem den Standort, die Häufigkeit der Nutzung einzelner *Apps* und die von den NutzerInnen aufgerufenen Internet-Seiten an den Hersteller. *Onavo* wurde inzwischen von *Facebook* übernommen.[92]

Adressbücher

Ebenfalls 2012 wurde aufgedeckt, dass die *Apps* der sozialen Netzwerke *Twitter*, *Path* und *Foursquare* die gesamten Adressbücher **ohne Nachfrage und Wissen** der NutzerInnen übertragen hatten– teils inklusive Name, E-Mail-Adresse, Telefonnummern und sogar Postadressen. Nach einem Sturm der Entrüstung und medialer Berichterstattung wurden die *Apps* in Hinblick auf Information und Zustimmung der NutzerInnen nachgebessert.

Erwartungshaltung und Realität

Den NutzerInnen ist oft nur sehr wenig bewusst, auf welche Daten *Apps* zugreifen – wie eine US-Studie über die Abweichungen zwischen Erwartungshaltung und Realität bei den 100 popu-

90 Cortesi, Aldo (2011): How UDIDs are used: a survey, 19.05.2011, abgerufen am 07.07.2014 von http://corte.si/posts/security/apple-udid-survey

91 Venne, Patrick Kollaten; Eikenberg, Ronald; Schmidt, Jürgen (2012): Selbstbedienungsladen Smartphone. c't, Heft 7/2012, S. 114.

92 Goel, Vindu (2013): Facebook Buys Israeli Maker of Data Compression Software for Mobile Web Effort, 14.10.2013, http://bits.blogs.nytimes.com/2013/10/14/facebook-acquires-onavo-and-a-foothold-in-israel (Abgerufen am 07.07.2013)

lärsten *Android-Apps* 2012[93] gezeigt hat. So waren beispielsweise 95% der 179 Studienteilnehmer davon überrascht, dass die Taschenlampen-App ***Brightest Flashlight*** auf Standort-Daten zugreift. 90% waren davon überrascht, dass die *App Background HD Wallpapers* auf das Adressbuch zugreift. Im Gegensatz dazu war aber kein einziger Teilnehmer (0%) davon überrascht, dass *Google Maps* auf die Standort-Daten zugreift. Insgesamt waren die StudienteilnehmerInnen in vielen Fällen davon überrascht, welche *Apps* auf Geräte-ID, Standort-Daten oder Adressbuch zugreifen. Die Studienautoren betrachten in Folge einen geringen Grad an Überraschung als eine Art von „informiertem Konsens".

Die Situation 2014

Obwohl das Thema medial immer wieder skandalisiert war, scheint sich die Situation seit 2010 sogar verschlimmert zu haben. *Appthority* untersucht regelmäßig die Reputation von *Apps* für den Unternehmenseinsatz. 2014 wurden erneut die je 200 populärsten *Apps* auf den Plattformen *iOS* und *Android* mit folgenden Resultaten auf **riskante Verhaltensmuster** hin untersucht (vgl. Appthority 2014):

Riskante Verhaltensweisen von Apps	Top 100 Apps Android		Top 100 Apps iOS	
	kostenlos	kostenpflichtig	kostenlos	kostenpflichtig
Zugriff auf Standort-Daten	82%	49%	50%	24%
Zugriff auf Geräte-ID, Identifikation von NutzerInnen	88%	65%	57%	28%
Zugriff auf Adressbuch	30%	14%	26%	8%
Datenübertragung an Werbenetzwerke	71%	38%	32%	16%
Datenübertragung an soziale Netzwerke	73%	43%	61%	53%
Datenübertragung an Frameworks und SDKs	38%	20%	31%	41%

Tabelle 12: *Riskante Verhaltensmuster von Smartphone-Apps. Quelle: Appthority, Summer 2014 App Reputation Report*

Riskante Apps

82% der kostenlosen Android-*Apps* und 50% der kostenlosen *iOS-Apps* greifen auf Standort-Daten zu, immer noch fast ein Drittel aller kostenlosen *Apps* greifen auf das Adressbuch zu. Viele *Apps* übertragen Daten an Werbenetzwerke und Datensammel-Unternehmen, die die gesammelten Daten oft wiederum weitergeben. Dabei werden bei den NutzerInnen nicht in allen Fällen Werbeanzeigen eingeblendet. In manchen Fällen werden die *App*-EntwicklerInnen nach der Menge der Daten bezahlt, die sie über NutzerInnen sammeln. Erstaunlicherweise übermitteln auch viele kostenpflichtige *Apps* Daten an Dritte. Viele EntwicklerInnen von *Apps* nutzen *Frameworks*, *Software Developer Kits* (SDK) oder Programmbibliotheken, viele davon sammeln ebenfalls umfangreiche NutzerInnendaten oder übertragen diese gar an *Analytics*-Anbieter wie *Google Analytics* oder *Flurry* weiter.

Nach einer anderen Untersuchung von 26 Datenschutzbehörden aus 19 Ländern aus dem Jahr 2014 greifen **31% von 1200 populären *Apps*** auf Daten zu, ohne dass dies für die eigentliche Funktion der *App* notwendig wäre (vgl. Office of the Privacy Commissioner of Canada 2014). 59% der *Apps* werden als bedenklich eingestuft, da sie die NutzerInnen nicht ausreichend darüber informieren, welche Daten genutzt und weitergegeben werden.

93 Lin, Jialiu; Sadeh, Norman M.; Amini, Shahriyar; Lindqvist, Janne; Hong, Jason I.; Zhang, Joy (2012): Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In: UbiComp, 2012. Abgerufen am 07.07.2014 von http://www.winlab.rutgers.edu/~janne/privacyasexpectations-ubicomp12-final.pdf

4.2. Fitness-Tracker und Wearables: Die Vermessung des Selbst

Was bis vor einigen Jahren nur bei chronisch Kranken oder im Spitzensport üblich war, wird nun nach und nach für breite Bevölkerungsschichten zum Alltag: Die **Optimierung des Selbst**[94] durch die kontinuierliche Vermessung der eigenen Vitalitäts- und Körperfunktionen mit verschiedenen Geräten von *Smartphone-Apps* über tragbare Sensoren bis zur vernetzten Waage. Unter Schlagwörtern wie **Quantified Self**[95], *Self Tracking* oder *Lifelogging* wird heute eine Vielzahl an Produkten zur digitalen Erfassung, Analyse und Auswertung von Körper- und Gesundheitsdaten vermarktet.

Körper- und Gesundheitsdaten

Dabei wird etwa die Anzahl der bewältigten Schritte, Pulswerte oder die Schlafdauer und -qualität gemessen – manchmal ergänzt durch laufende Erfassung des Standorts via GPS-Sensor. Viele dieser Anwendungen bieten Unterstützung bei der Erfassung von **Sportaktivitäten, Gewicht, Ernährungsgewohnheiten**, manche auch von **weiblichem Zyklus, Alkohol- oder Nikotinkonsum** oder sogar von **Stimmung** und **psychischem Wohlbefinden**. Die meisten tragbaren Fitness-Tracker – im englischen Sprachraum oft als „Wearables" bezeichnet - messen die körperliche Aktivität mit einem Beschleunigungssensor[96], der Richtung und Intensität von Bewegungen erkennt.

Vielfältige Sensoren

Die gemessenen Werte werden mehr oder weniger genau in **Schritte**, **Kalorienverbrauch**, bewältigte **Strecken** und **Schlafdauer bzw. -qualität** umgerechnet (z.B. bei den Fitness-Armbändern *Fitbit Flex* oder *Jawbone Up*). Andere Produkte bieten zusätzlich einen Sensor für die Messung von **Puls** bzw. Herzfrequenz (z.B. *Samsung Gear Fit*, *Garmin Vivofit*, *POLAR Loop*), manche einen **Höhensensor** (*Fitbit The One*, *Withings Pulse O2*, *Runtastic RUNGPS1*) oder sogar Sensoren für **Hautwiderstand oder Temperatur** (z.B. *Basis B1*). Die gemessenen Daten sind in Folge via Web-Plattform oder *Smartphone-App* zugänglich und können von den NutzerInnen mit weiteren Informationen angereichert werden – etwa mit Angaben zu **Ernährungsverhalte**n (umgerechnet in Kalorienaufnahme), **Gewicht**, **Körpermaße**, **Blutdruck** und **Blutzucker**. Durch die Vorstellung der *Apple Watch* – einer sogenannten **Smartwatch** mit Bewegungs- und Puls-Sensoren - hat der Hype um *Wearables* 2014 einen neuen Höhepunkt erreicht.

Die Erfassung des eigenen Alltags…

Auf der Website *quantifiedself.com*[97] findet sich ein Verzeichnis von über 500 derartiger Tools, die sich nicht auf die Messung von Körperfunktionen beschränken. Von Anwendungen zur Erfassung und Verbesserung von **Produktivität** (z.B. Todo-Listen-*Apps*), **Lernfortschritten** oder **psychischem Wohlbefinden** bis zur Analyse des eigenen Online-Verhaltens oder der eigenen sozialen Netzwerke werden dabei die unterschiedlichsten Lebensbereiche abgedeckt – teils mit dem Ziel der möglichst weitgehenden Erfassung des eigenen Alltags. In einem weiteren Sinn werden auch klassische Social Media Plattformen wie *Facebook*, *Twitter* oder *Instagram* unter dem Paradigma des *Self Tracking* genutzt.

…wird Mainstream

2007 war es nur eine kleine Community, die sich rund um die Plattform *quantifiedself.com* über die Vermessung des Selbst und geeignete Hilfsmittel ausgetauscht hat. Mitbegründer der Plattform ist Gary Wolf, der seit der Veröffentlichung seines Manifests „The Data-Driven Life"[98] als

94 Friedrichs, Julia (2013): Selbstoptimierung. Das tollere Ich. Zeit Magazin, 12.08.2013. Abgerufen am 04.07.2014 von http://www.zeit.de/2013/33/selbstoptimierung-leistungssteigerung-apps

95 http://de.wikipedia.org/wiki/Quantified_Self

96 http://de.wikipedia.org/wiki/Beschleunigungssensor

97 http://quantifiedself.com (Abgerufen am 04.07.2014)

98 Wolf, Gary (2010): The Data-Driven Life. New York Times, 02.05.2010. Abgerufen am 04.07.2014 von http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?pagewanted=all

Vordenker der Bewegung gilt. 2012 wurden laut einer Markteinschätzung von IHS[99] etwa 40 Millionen Geräte[100] ausgeliefert, für **2018 werden an die 80 Millionen prognostiziert**. Für 2018 wird erwartet, dass mit *Wearables* insgesamt weltweit ein Umsatz von 30 Mrd. Dollar erwirtschaftet wird[101]. Dan Rose - Vizepräsident für Partnerschaften bei *Facebook* – bezeichnete Fitness nach Musik und Büchern als einen der wichtigsten digitalen Trends 2013[102].

Optimierung des Selbst

Eine wesentliche Komponente bei der Vermessung des Selbst ist die Auswertung der Rohdaten, die via Web-Plattform oder *Smartphone-App* in Form von Tabellen, Charts und Diagrammen bereitgestellt werden. Die NutzerInnen werden dazu motiviert, die Geräte oft einzusetzen, damit die Auswertungen möglichst aussagekräftig sind. Ziel ist die Beobachtung und Optimierung des eigenen Körpers in Hinblick auf **Schönheitsideale** (Figur, Gewicht), aber auch auf **gesundheitliche Aspekte**. Gesellschaftlich positiv besetzte Konzepte wie *Fitness* oder *Wellness* versprechen gleichermaßen Ausgeglichenheit, Leistungsfähigkeit, Glück und Spaß.

Ziele setzen!

Alle derartigen Anwendungen bieten die Möglichkeit, **Zielwerte** zu setzen – beispielsweise eine bestimmte wöchentliche Laufstrecke oder eine bestimmte Anzahl der täglich zu bewältigenden Schritte. Das Erreichen der Zielwerte wird mit Aktivitäts-Punkten, Trophäen oder virtuellen Abzeichen belohnt, der verbleibende Weg zum Ziel durch Fortschrittsanzeigen visualisiert. Zusätzlich werden die NutzerInnen dazu motiviert, ihre Auswertungen und Erfolge mit anderen zu teilen. Meist besteht auch die Möglichkeit, die gemessenen Daten via *Social Media* zu teilen oder auf einer öffentlichen Profilseite zur Verfügung zu stellen – in manchen Fällen ist das sogar die Standard-Einstellung.

4.2.1. Exkurs: Beeinflussung von Verhalten durch „Gamification"

Beinahe alle Fitness-*Apps* setzen auf das in den letzten Jahren oft diskutierte Konzept der „Gamification", also auf den **Einsatz von spieltypischen Elementen in spielfremden Kontexten** (vgl. Deterding et al 2011) zur Beeinflussung der Verhaltensweisen[103] der NutzerInnen sowie zur Steigerung von Beteiligung und Engagement[104]. Dabei werden mehr oder weniger komplexe „Spielregeln" vorgegeben, die durch Mechaniken ergänzt werden, die erwünschtes Verhalten belohnen - oder seltener - unerwünschtes Verhalten sanktionieren. Beispiele dafür sind laut Breuer:

Erwünschtes Verhalten belohnen…

- Die NutzerInnen erhalten kontinuierlich Punkte, wenn sie bestimmte Tätigkeiten ausüben
- Die NutzerInnen erhalten bei Zwischenzielen Auszeichnungen, Orden, Trophäen oder Badges
- Fortschrittsanzeigen, die in Form von Balken, Kreisen oder Prozent-Zahlen den Weg bis zum Ziel anzeigen

---

99 Walker, Shane. (2013). Wearable Technology—Market Assessment. IHS Whitepaper. S. 16. Abgerufen am 04.07.2014 von http://www.ihs.com/pdfs/Wearable-Technology-sep-2013.pdf

100 Die Zahl bezieht sich auf „Performance Monitors" inkl. Herzfrequenz-Tracker, Sport- und Laufcomputer, Aktivitäts-Tracker, Fahrradcomputer und Schrittzähler

101 HIS (2014): Wearable electronics: The next must-have fashion accessory. Q1/2014. Abgerufen am 19.09.2014 von http://www.ihs.com/tl/quarterly/insights/fashion-accessory.aspx

102 Sullivan, Danny (2013): For Facebook, „2013 Will Be The Year Of Music, Books, Fitness". Marketing Land, 12.02.2013. Abgerufen am 04.07.2014 von http://marketingland.com/facebook-dan-rose-33219

103 Breuer, Markus (2011): Was ist Gamification? Abgerufen am 05.07.2014 von http://intelligent-gamification.de/2011/05/11/was-ist-gamification

104 Fitz-Walter, Zachary; Tjondronegoro, Dian (2011): Exploring the Opportunities and Challenges of Using Mobile Sensing for Gamification.. In: UbiComp 11: Proceedings of the 2011 ACM Conference on Ubiquitous Computing, ACM Press, Beijing, pp. 1-5. Abgerufen am 05.07.2014 von http://eprints.qut.edu.au/48632

- Belohnungen in Form von limitierten virtuelle Gegenständen bzw. Statussymbolen
- Rangstufen bzw. „Levels“, die nacheinander erreicht werden können und nach bestimmten Regeln vergeben werden (z.B. Punkte, Dauer der Nutzung)
- Ranglisten bzw. „Leaderboards“, in denen die besten NutzerInnen aufscheinen
- Zeitdruck, der bewirkt, dass Belohnungen nur innerhalb bestimmter Zeiträume erreicht werden können
- Mechanismen, die die soziale Interaktion oder den Wettbewerb zwischen NutzerInnen stärken
- Puzzles, Rätsel oder andere kleine Herausforderungen als zusätzliche Hürden
- NutzerInnen bewerten sich gegenseitig

Spielmechaniken im Marketing

Spielmechaniken wie diese sind nicht nur von Computerspielen bekannt, sondern auch von klassischen Brett- oder Kartenspielen. Auch im Marketing werden derartige Mechaniken schon lange genutzt (z.B. Bonuskarten im Handel, Vielfliegerprogramme, „Happy Hour“ in der Gastronomie, Sammelkarten oder -aufkleber, Autoaufkleber für die Teilnahme an einem Gewinnspiel). Im Online-Bereich spielen die unter dem Hype-Begriff „Gamification“ gefassten Konzepte aber eine besonders prominente Rolle – von der Anzahl der *Friends* oder *Likes* bei *Facebook*, der *Followers* oder *Tweets* bei *Twitter*, der *Badges* bzw. Abzeichen bei *Foursquare* oder der Bewertungen bei *eBay*. Im Online-Marketing wird *Gamification* generell immer mehr eingesetzt, um KundInnen zu gewinnen und sie zu binden.

4.2.2. Beispiel: Fitbit

Fitbit[105] wurde 2007 gegründet und ist laut dem US-Marktforschungsunternehmen *Canalys* mit fast 50% Marktanteil im ersten Quartal 2014[106] globaler Marktführer bei Fitness-Armbändern. Das US-Unternehmen bietet aktuell mit den Aktivitäts- und Schlaf-Trackern *Flex*, *Zip* und *One* sowie der vernetzten Waage *Aria* vier Hardware-Produkte an. *Fitbit Flex* ist ein Aktivitäts-Tracker in Armband-Form, misst die Aktivität der NutzerInnen mit einem Beschleunigungssensor und überträgt die Rohdaten via *Bluetooth* und auf *Smartphone* oder Rechner installierter Software an die Server von *Fitbit,* die laut *Privacy Policy*[107] von *Fitbit* **in den USA** liegen.

Ziele erreichen!

Aus den Aktivitäts-Daten werden die gegangenen Schritte, zurückgelegte Strecke, aktive Minuten, verbrannte Kalorien, geschlafene Stunden und Schlafqualität berechnet. Zusätzlich können die NutzerInnen manuell täglich Gewicht, Herzfrequenz, Blutdruck, Blutzucker und ihre täglichen Mahlzeiten in Form von einzelnen Lebensmitteln online eingeben. In einem „Tagebuch“ können Stimmung oder Allergien eingetragen werden. Aus allen gemessenen und eingetragenen Daten werden verschiedenste Grafiken und Diagramme generiert. Die NutzerInnen können sich **Ziele setzen** (z.B. Gewichtsabnahme), mehrwöchige Fitnesspläne einrichten oder „Abzeichen“ erhalten – beispielsweise für 10.000 tägliche Schritte oder eine bewältigte Gesamtstrecke von 80 Kilometern. Verschiedene Fortschrittsbalken zeigen an, wie viel an Aktivität noch fehlt, um die Zielwerte zu erreichen. Auch am Gerät selbst stehen rudimentäre Fortschrittsanzeigen zur Verfügung.

Sozialer Wettbewerb

Außerdem sind viele Funktionen eines **sozialen Netzwerks** in die Software integriert. Die NutzerInnen erhalten eine öffentlich zugängliche Profilseite mit Pseudonym und Profilfoto, in der

105 http://www.fitbit.com (Abgerufen am 05.07.2014)
106 http://www.canalys.com/newsroom/fitbit-accounted-nearly-half-global-wearable-band-shipments-q1-2014 (abgerufen am 05.07.014)
107 Fitbit-Datenschutzerklärung vom 10.08.2014: http://www.fitbit.com/de/privacy (abgerufen am 20.09.2014)

Standard-Einstellung werden Schritte, Strecke und Fortschrittsanzeigen öffentlich dargestellt. Via E-Mail können „Freunde“ eingeladen werden, die je nach Datenschutzeinstellungen ausführlichere Informationen wie Ernährung oder Schlafdauer angezeigt bekommen. Mehrere Funktionen motivieren zum Wettbewerb mit „Freunden“ oder mit anderen Fitbit-NutzerInnen in Foren oder Gruppen. Aktivitäten können via *Facebook* oder *Twitter* geteilt und mit anderen *Apps* verknüpft oder synchronisiert werden [108] – beispielsweise mit der Gesundheitsdaten-Plattform *Microsoft HealthVault,* mit einem Account bei *Weight Watchers* oder mit der populären Fitness- und Kalorienzähler-*App MyFitnessPal*.

Weitergabe von Daten an Dritte

In der Datenschutzerklärung von *Fitbit* wird darauf hingewiesen, dass NutzerInnendaten bei Synchronisierung mit einer Dritt-*App* der *Privacy Policy* der Dritt-*App* unterliegen würden. Dazu könne *Fitbit* etwa im Falle eines Verkaufs, einer Fusion, einer Umstrukturierung oder eines Verkaufs von Teilen des Unternehmens **personenbezogene Daten verkaufen oder weitergeben**[109]. Darüber hinaus werden in der Datenschutzerklärung mehrere in *Fitbit* integrierte Dritt-Services erwähnt, an die NutzerInnendaten bei der Einbindung von *Widgets* oder Werbe-, Tracking- oder Analyse-Zwecken übertragen werden – unter anderem an: *ApNexus*, *DataXu*, *DoubleClick* (*Google*), *DoubleClick Floodlight* (*Google*), *Google Adwords*, *Google Analytics*, *Optimizely* und *MixPanel.* Die Interaktionen der NutzerInnen mit diesen Dritt-Services würden nicht der *Privacy Policy* von *Fitbit* unterliegen, sondern der ***Privacy Policy* der Dritt-Services**. Die NutzerInnen müssten also vor Gebrauch theoretisch mindestens neun mehrere Seiten lange Datenschutzrichtlinien lesen, um zu verstehen, auf welche Art und Weise *Fitbit* ihre persönlichen Daten verarbeitet.

4.2.3. Weitergabe von Gesundheitsdaten an Unternehmen und Versicherungen

Angebote an Versicherungen

Auf der Website des Fitness-Trackers *Fitbit* werden Angebote für „Arbeitgeber“ sowie für „Versicherungsunternehmen und Gesundheitsbranche“ mit folgender Formulierung beworben: „Erzielte Fortschritte im Laufe der Zeit anhand zuverlässiger Daten messen“ [110] (siehe Abb. 1). Dazu werden den Unternehmen durch Gesundheitsprogramme „weniger Krankheitstage“, „weniger gesundheitsbezogene Kosten“ und „höhere Mitarbeiterproduktivität“ versprochen. Hinter dem Angebot an ArbeitgeberInnen steht die Situation in den USA, wo 62% der Arbeitnehmer durch hauptsächlich von ArbeitgeberInnen bezahlte Prämien krankenversichert sind[111].

Fitbit verkauft die Geräte laut *Forbes* (vgl. Olson 2014[112]) an „tausende“ Firmen mit Rabatt - da-

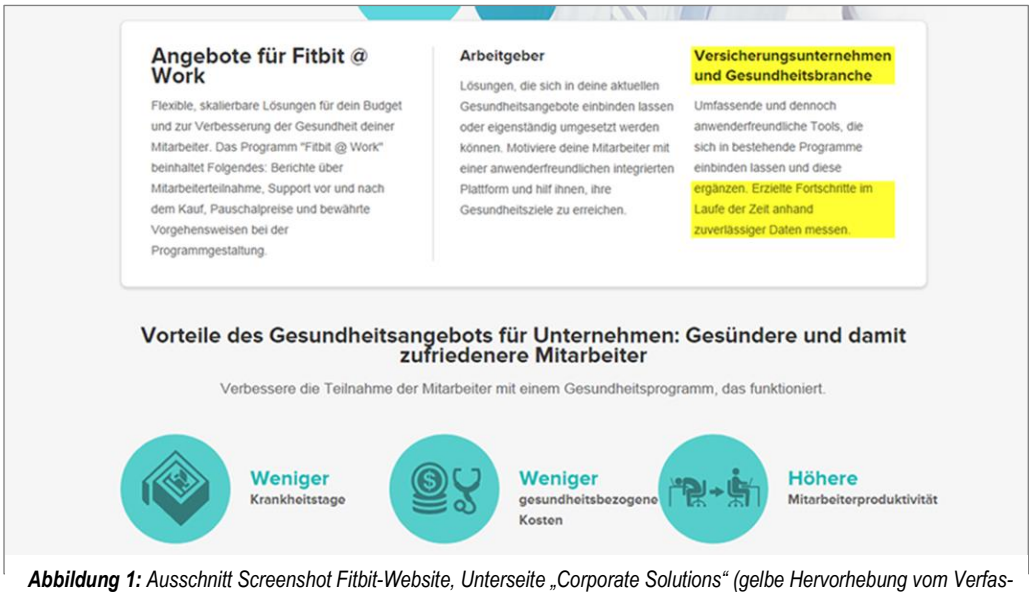

Abbildung 1: *Ausschnitt Screenshot Fitbit-Website, Unterseite „Corporate Solutions“ (gelbe Hervorhebung vom Verfasser)*

Betriebliche Vorsorgeprogramme

runter an große Unternehmen wie *AutoDesk* und *BP* - die die Tracker im Rahmen **betrieblicher Vorsorgeprogramme** kostenlos an ihre MitarbeiterInnen weitergeben. Spezielle Zusatz-Software ermöglicht es, dass Abteilungen miteinander konkurrieren. Der CEO von *Fitbit* sagt, dies sei einer ihrer am schnellsten wachsenden Geschäftsbereiche. *Bloomberg* (vgl. Satariano 2014[113]) zitiert eine Unternehmenssprecherin mit der Aussage, dass *Fitbit* eine eigene Verkaufsabteilung für Unternehmen und Versicherungen eingerichtet hätte.

Krankenversicherung: 1.200 Dollar Ersparnis

Bei der US-Firma *Appirio* nehmen laut *Bloomberg* 40% bzw. rund **1.000 Angestellte** an einem freiwilligen Vorsorgeprogramm statt, das die Zurverfügungstellung ihrer *Fitbit*-Daten inkludiert. Der CEO von *Appirio* wird mit der Aussage zitiert, dass sein Unternehmen dadurch mit deren Versicherung eine **Ermäßigung von 300.000 Dollar** ausverhandeln konnte – bei jährlichen Krankenversicherungskosten von etwa 5 Millionen Dollar. Im Jahr 2013 haben sich laut *Forbes* (vgl. Olson 2014b[114]) **14.000 Angestellte des Ölkonzerns *BP*** dafür entschieden, einen kostenlosen *Fitbit-Tracker* zu benutzen. Wer von diesen Angestellten im Jahr 2013 **eine Million Schritte** bewältigte, bekam „Wellness-Punkte" und bezahlte in Folge eine geringere Prämie für die Krankenversicherung. Das Unternehmen *BP* ist für die Krankenversicherung ihrer Angestellten zuständig und außerdem „selbstversichert" - das bedeutet, *BP* nutzt keine externe Versicherung. Laut *Bloomberg* hat sich einer der *BP*-Mitarbeiter durch die Teilnahme an diesem Programm ganze **1.200 Dollar** bei der jährlichen Krankenversicherungsprämie erspart. Dies ist ein durchaus starker Anreiz und bedeutet umgekehrt: Wer nicht teilgenommen oder das „spielerische" Ziel nicht erreicht hat, wird bestraft und bezahlt spürbar mehr. Um das Ziel von einer Million Schritten zu erreichen, muss das Gerät relativ häufig getragen werden.

Verwaltung der Daten durch neutrale Parteien

Die im Rahmen der betrieblichen *Fitbit*-Vorsorgeprogramme gesammelten Gesundheitsdaten der MitarbeiterInnen werden dabei immerhin von externen Unternehmen wie ***StayWell*** als „neutrale Parteien" verwaltet[115]. Die Firma *StayWell* beschreibt sich allerdings selbst als „population health management company", bietet unter anderem „incentive designs to motivate" an und wirbt mit Sätzen wie: „Attract them. We create a supportive ecosystem that prepares people for behavior change"[116]. Diese „neutrale Partei" beschäftigt sich also hauptsächlich mit „Anreizen zur Verhaltensänderung" im Gesundheitsbereich - die Vertrauenswürdigkeit von *StayWell* als Datentreuhänder könnte zumindest in Frage gestellt werden.

Gerät gegen Gesundheitsdaten?

Manche rechnen damit, dass Versicherungen Fitness-Tracker in Zukunft durch **Quersubventionsmodelle** vermarkten könnten, bei dem die Geräte bei vertraglicher Bindung „kostenlos" an die KonsumentInnen abgegeben werden – ähnlich wie die Vertriebskonzepte von Mobilfunk-Netzbetreibern, bei denen „kostenlose" *Smartphones* gegen vertragliche Bindung angeboten werden[117]. Florian Gschwandtner - CEO des österreichischen Fitness-*App*-Anbieters ***Runtastic*** – hat laut *Forbes* bereits mehrmals mit österreichischen und US-Versicherungen gesprochen und wird mit der Aussage zitiert, dass die diese zwar nicht nach einem Partner Ausschau gehal-

---

113 Satariano, Adam (2014): Wear This Device So the Boss Knows You're Losing Weight. Bloomberg. Abgerufen am 19.09.2014 von http://www.bloomberg.com/news/2014-08-21/wear-this-device-so-the-boss-knows-you-re-losing-weight.html

114 Olson, Parmy (2014b): Wearable Tech Is Plugging Into Health Insurance. Forbes, 19.06.2014. Abgerufen am 05.07.2014 von http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/

115 StayWell (2014): Case Study. Abgerufen am 05.07.2014 von http://staywell.com/wp-content/uploads/2014/01/StayWell-BP-CaseStudy_Jan2014.pdf

116 http://staywell.com/what-we-do/our-approach-workplace-wellness-programs (Abgerufen am 19.09.2014)

117 Seitz, Patrick (2014): Apple may seek health insurer subsidies for iWatch fitness bands. investors.com, 4.11.2014. Abgerufen am 19.09.2014 von http://news.investors.com/technology-click/041114-696987-apple-iwatch-could-be-subsidized-by-insurance-providers.htm

ten hätten, aber jedenfalls Zugriff auf die von derartigen *Apps* generierten Fitness-Daten begehren würden (vgl. Olson 2014b). Nach Aussage eines anderen Experten wären insbesondere Blutzucker-Sensoren für den Gesundheitssektor besonders interessant, denn diese würden einen direkten Einblick in das Ernährungsverhalten bieten.

Kleine Belohnungen

Große **US-Versicherungsunternehmen** wie *United Health*, *Humana* oder *Cigna* haben laut *Bloomberg* inzwischen Programme gestartet, die *Wearables* integrieren. Bei Teilnahme erhalten die KonsumentInnen die Geräte und ihre Aktivitätsdaten werden an ein Online-System übertragen. Der US-Versicherer *Humana* bietet seinen 13 Millionen KundInnen mit *HumanaVitality*[118] etwa ein Programm, bei dem die KonsumentInnen bei Erreichen bestimmter Fitness-Ziele kleine Belohnungen wie Einkaufsgutscheine oder Kinotickets erhalten können. Es ist wahrscheinlich nur mehr eine Frage der Zeit, bis auch KonsumentInnen in den USA direkte Rabatte auf Versicherungsprämien erhalten.

Strafen statt Belohnungen

Andere experimentieren mit Strafen anstatt von Belohnungen: Das US-Startup ***StickK***[119] bietet etwa eine Software an, die die Daten von *Wearables* einbezieht – und mit der nicht etwa „Wellness-Punkte" gesammelt werden, sondern umgekehrt Punkte abgezogen werden, wenn die NutzerInnen die vorgegebenen Aktivitäts-Ziele nicht erreichen. Deren Angebot für Privatpersonen basiert auf einer Art „Vertrag", in dem sich die NutzerInnen dazu verpflichten, bei Nicht-Erreichen ihrer Fitness-Ziele einen bestimmten Betrag an eine zuvor festgelegte Organisation zu spenden. Laut *Forbes* arbeitet *StickK* auch für Firmen – unter anderem für drei „Fortune 500"-Unternehmen (vgl. Olson 2014b).

Auch in Deutschland wurden Fitness-Tracker bereits in ganz spezifischen Situationen eingesetzt: 2013 hat das Jobcenter Brandenburg **15 langzeitarbeitslose Hartz-IV-EmpfängerInnen** mit Schrittzählern ausgestattet, Ziel war das „spielerische" Erreichen von 270.000 Schritten.[120]

118 https://www.humana.com/vitality/ (Abgerufen am 19.09.2014)

119 http://en.wikipedia.org/wiki/StickK

120 Osang, Alexander (2013): 5 724 512 Schritte. Der Spiegel, 09.02.2013. Abgerufen am 19.09.2014 von http://www.spiegel.de/spiegel/print/d-90931289.html

4.3. Günstigere Versicherung mit Überwachungs-Box im Auto

„Werbung ist zum nativen Geschäftsmodell für das Internet geworden. Ich denke, dass Versicherung zum nativen Geschäftsmodell für das Internet der Dinge wird“
[121]

Tim O'Reilly, 2014

Fahrzeug-Telemetrie ist ein Wachstumsmarkt. Dabei wird eine Box in das Auto eingebaut, die rund um die Uhr das Fahrzeug überwacht - und Informationen zu Position, Uhrzeiten, Geschwindigkeiten oder zu Brems- und Beschleunigungswerten an verschiedene Dienstleister überträgt. Unter Schlagwörtern wie „vernetztes Auto“ oder „Smart Car“ wird die Entwicklung seit Jahren vorangetrieben.

International bereits etabliert

International haben sich Versicherungstarife, die die Auswertung dieser Daten in die Preisgestaltung einbeziehen, schon etabliert. In einer Studie einer industrienahen Beratungsfirma[122] über ***Usage-based Insurance*** und ***Insurance Telematics*** werden weltweit 95 Angebote im B2C-Bereich angeführt - die meisten davon in den USA, UK, Italien, Frankreich, Südafrika und Spanien. Insgesamt werden global **5 Millionen** derartige Versicherungspolizzen geschätzt, für 2020 werden über 100 Millionen Polizzen prognostiziert. Das Angebot „Snapshot“ des US-Versicherers Progressive wurde laut Eigenangabe bisher in 2 Millionen Autos genutzt[123].

Österreich und Deutschland

Auch in Deutschland gibt es bisher ein diesbezügliches Produkt (siehe folgendes Kapitel), in **Österreich** bietet die *Uniqua*-Versicherung das Produkt „SafeLine“ an, das die Höhe der Prämie von der gemessenen Kilometerleistung abhängig macht[124]. Das ins Fahrzeug eingebaute Gerät bietet zwar ebenfalls GPS-Ortung im Fall eines Unfalls, bisher wird aber das über die Kilometerleistung hinausgehende Fahrverhalten nicht in die Prämienberechnung einbezogen. Laut Eigenangabe wird das System bereits von 50.000 KundInnen genutzt[125].

4.3.1. Beispiel: Sparkassen DirektVersicherung

Von November 2013 an konnte bei der deutschen „Sparkassen DirektVersicherung“ ein Tarif[126] gewählt werden, für den eine „Mess- und Telematikbox“ im Auto eingebaut werden muss, die eine Rundum-Überwachung des Fahrverhaltens beinahe in Echtzeit ermöglicht und bei Erreichen bestimmter Zielwerte einen Rabatt in Aussicht stellt. Die Box ist mit GPS- und Beschleunigungssensoren ausgestattet und sendet alle 20 Sekunden Rohdaten zu **Position, Uhrzeit, Geschwindigkeit** des Fahrzeugs sowie zu **Brems- und Beschleunigungswerten** an die Zentrale.

---

121 Myslewski, Rik (2014): The Internet of Things helps insurance firms reward, punish. The Register, 24.05.2014. Abgerufen am 19.09.2014 von http://www.theregister.co.uk/2014/05/23/the_internet_of_things_helps_insurance_firms_reward_punish

122 Ptolemus Consulting Group (2013): Usage-based Insurance Global Study. Free Abstract. S. 7. Abgerufen am 30.06.2014 von http://www.ptolemus.com/content/uploads/2013/10/UBI-Global-Study-Free-Abstract1.pdf

123 http://www.progressive.com/newsroom/article/2014/march/snapshot-ten-billion-mile (Abgerufen am 30.06.2014)

124 http://www.uniqa.at/uniqaat/cms/geschaeftskunden/kfzversicherung/UNIQA-SafeLine.de.xhtml (Abgerufen am 30.06.2014)

125 http://www.uniqagroup.com/gruppe/versicherung/press/press_release/archive/2012/pa_50000_safeliner.de.html (Abgerufen am 30.06.2014)

126 https://www.sparkassen-direkt.de/telematik/mehr.html (Abgerufen am 30.06.2014)

Daraus werden etwa die zurückgelegten Kilometer berechnet, durch die Verknüpfung mit Kartenmaterial werden **Geschwindigkeitsübertretungen** erkannt.

Punktebewertung für Fahrverhalten

Aus den aufgezeichneten Rohdaten wird ein **Risikoprofil** errechnet, das sich aus einzelnen Score-Werten für Geschwindigkeit, Fahrweise, Nachtfahrten und Stadtfahrten zusammensetzt (vgl. Abb. 2). Wer „risikoarm" fährt, bekommt im folgenden Jahr einen **Abschlag von 5%** auf die Versicherungsprämie. Wer einige Male die erlaubte Geschwindigkeit überschreitet, zu oft abrupt beschleunigt und bremst oder zu viel in der Nacht oder im städtischen Bereich fährt, verliert diesen Rabatt. Um die Ermäßigung zu erhalten, muss am Jahresende bei einem Ausgangswert von 100 ein Gesamt-Score von 80 erreicht werden, der sich aus den gewichteten Einzel-Scores zusammensetzt. Die möglichen Punkteabzüge aufgrund **falschen Fahrverhaltens** werden mit Sicherheit und Ökologie begründet und auf der Website wie folgt dargestellt[127]:

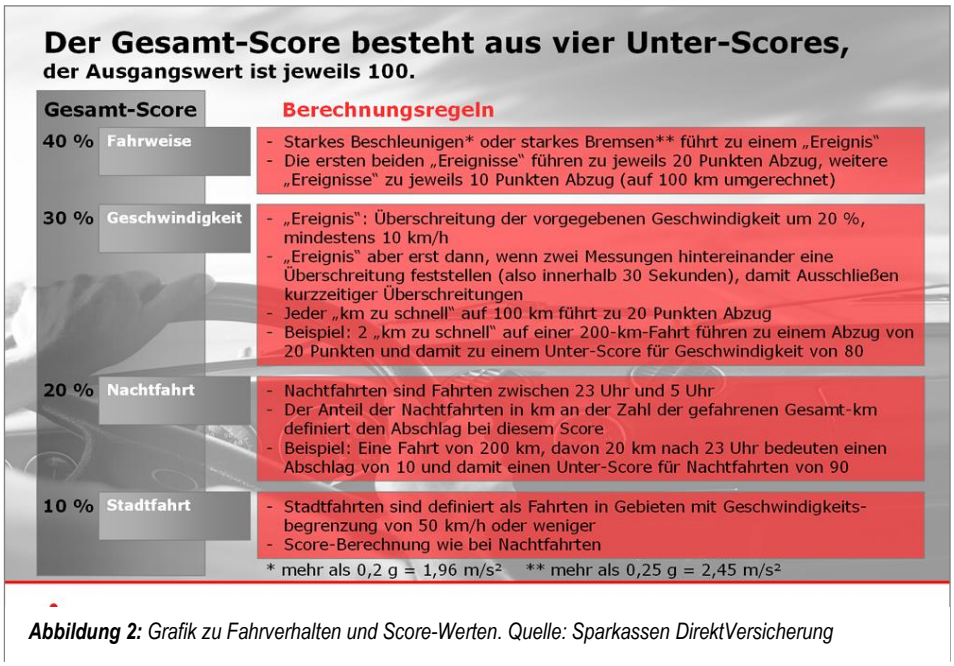

Abbildung 2: *Grafik zu Fahrverhalten und Score-Werten. Quelle: Sparkassen DirektVersicherung*

Vor- und Nachteile

Der Tarif wird damit beworben, dass durch die Überwachung der Beschleunigungswerte bei Unfällen automatisch eine Notfallstelle alarmiert wird und das Fahrzeug im Fall eines Diebstahls geortet werden kann. Außerdem können die KundInnen alle Details zu Fahrverhalten und gefahrenen Strecken via Online-Portal und *App* selbst einsehen. Gleichzeitig wird eine **Nachbelastung** „gemäß dem für das Jahr gültigen Kfz-Versicherungstarif" in Aussicht gestellt, wenn die „im Jahr gefahrene km-Zahl mit mindestens 15%" über der „im Rahmen der Kfz-Versicherung angegebenen km-Zahl liegt". Aus den umfangreichen, aber etwas unübersichtlichen Informationen zu **Datenschutz**[128] und **Speicherung der Daten**[129] geht hervor, dass die Rohdaten an ein Serverzentrum in London übermittelt werden, dass von der britischen Firma *Masternaut* im Auftrag des spanischen Telekom-Konzerns *Telefónica* betrieben wird. Es wird mehrfach betont, dass die *DirektVersicherung* keinen Zugriff auf die Rohdaten hätte, sondern nur auf die monatlichen Score-Werte und die gefahrenen Kilometer. Die vergleichsweise ausführliche Darstellung dieser Abläufe[130] kann allerdings nicht darüber hinwegtäuschen, dass das **eigentliche Potenzial** gar nicht in

127 https://www.sparkassen-direkt.de/fileadmin/images/divers/Telematik/2014-01-29_score-logik.jpg (Abgerufen am 30.06.2014)
128 https://www.sparkassen-direkt.de/telematik/merkblatt/datenschutz.html (Abgerufen am 30.06.2014)
129 https://www.sparkassen-direkt.de/fileadmin/pdf/datenfluss.im.ueberblick.pdf (Abgerufen am 30.06.2014)
130 https://www.sparkassen-direkt.de/fileadmin/pdf/getrennte.datenkreise.pdf (Abgerufen am 30.06.2014)

den Rohdaten liegt, sondern gerade in den aggregierten Daten und Scores. Weitere Anmerkungen zu diesem Angebot:

Fragwürdige Kriterien und Anreize

- Der mögliche Rabatt von 5% erscheint angesichts der dafür in Kauf zu nehmenden Rund-um-Überwachung geringfügig – und nicht zuletzt auch angesichts der möglichen Mehrkosten bei Überschreitung der gemessenen Kilometerleistung.
- Die Kriterien für die Punkteabzüge sind willkürlich angesetzt, schon wenige Abweichungen beim Fahrverhalten können den Rabatt zu Nichte machen. Die Punkteabzüge etwa bei „Nachtfahrten" bestrafen generell das Fahren in der Nacht.
- Außerdem werden falsche bzw. sogar gefährliche Anreize gegeben: Das System kann etwa keinesfalls zwischen aus Sicherheitsgründen notwendigen und selbstgewählten starken Bremsvorgängen unterscheiden.

„Riskante Alleinarbeit"

Telematikbox und Server-Infrastruktur des Angebots der „DirektVersicherung" werden etwa Logistik-Dienstleister *Masternaut* zur Verfügung gestellt, der sein Produkt „Risk Director" mit folgendem Satz bewirbt: „Arbeitsbezogene Fahrten und Alleinarbeit zählen europaweit zu den größten unkontrollierten Risiken."[131] Die Benennung von „Alleinarbeit" als ein von ArbeitgeberInnen zu überwachendes „Risiko" ist bezeichnend. Generell werden derartige Technologien bereits heute zur **Überwachung von ArbeitnehmerInnen** in den Bereichen Logistik, Zustellung und Außendienst eingesetzt.

Der beschriebene Tarif der *DirektVersicherung* wurde laut Eigenangabe bisher an nur 1.000 KundInnen verkauft und ist aktuell vergriffen, Interessenten können sich laut Website aber in eine Warteliste eintragen lassen (Stand Oktober 2014).

Offene Fragen und Implikationen

Wer bekommt Zugriff?

Die Player in diesem Bereich sind nicht nur Gerätehersteller, Service-Anbieter, Telekom-Konzerne und Versicherungen, sondern vor allem auch die Fahrzeughersteller selbst. Neuwagen haben die benötigten Sensoren meist bereits an Bord. Internationale Angebote setzen teils anstatt auf vollwertige Telemetrie-Boxen auf ***Smartphone-Apps***, die mit speziellen Schnittstellen mit dem Fahrzeug-Computer verbunden werden können. Einige Lösungen bieten sekundengenaue Datenübertragung oder weitergehende Auswertungen von Kurvenbeschleunigung bis Spritverbrauch. Mittelfristig ist denkbar, dass derartige Versicherungstarife **nicht mehr optional sind, sondern verpflichtend**. Außerdem könnten sich neben Behörden (Maut, Straßenverkehrsordnung von Einbahnregeln bis Geschwindigkeitsbeschränkungen) auch unterschiedliche andere Unternehmen für diese Daten interessieren. Diese Unternehmen könnten beispielsweise Anreize in Form von Ermäßigungen oder Belohnungen für eine freiwillige Zurverfügungstellung der aggregierten Score-Werte anbieten.

Ab dem Jahr 2015 wird das umstrittene gesetzliche Notrufsystem ***eCall*** europaweit in allen neuzugelassenen Fahrzeugmodellen Pflicht sein[132], das all die Sensoren an Bord hat, die auch für die beschriebenen Versicherungsmodelle benötigt werden. Auch hier stellen sich die Fragen: Wie sicher ist das System? Und wer bekommt Zugriff?

131 http://www.masternaut.com/de/produkte/masternaut-risk-director (Abgerufen am 30.06.2014)

132 Wiesmüller, Max (2014): Notrufsystem eCall ist ab 2015 Pflicht in Autos. Die Welt, 17.09.2014. Abgerufen am 20.09.2014 von http://www.welt.de/wirtschaft/webwelt/article132332877/Notrufsystem-eCall-ist-ab-2015-Pflicht-in-Autos.html

4.4. Allgegenwärtige Überwachung im Internet der Dinge?

Der Begriff „Internet of Things“ bzw. **Internet der Dinge** geht auf Kevin Ashton[133] zurück und bezeichnet eine „technische Vision, Objekte beliebiger Art in ein universales digitales Netz zu integrieren“ (vgl. Gabriel et al 010) In dieser Vorstellung werden zukünftig eine Vielzahl von Objekten - von Kleidungsstücken und Konsumgütern über Stromzähler bis hin zu Autos - eine eigene „Identität“ im Netzwerk haben und „in der Lage sein, durch integrierte Sensoren ihre Umgebung wahrzunehmen, Informationen zu verarbeiten, mit anderen Objekten und Netzwerken zu kommunizieren und selbst auch Aktionen auszulösen.“ Als Vorreiter gilt die **Logistik**, in der inzwischen große Teile des globalen Warenverkehrs vom Paket- bis zum Containerversand digital gesteuert und kontrolliert werden. Auch in Bereichen wie Fertigung, Gebäudetechnik, Autoverkehr oder Energieversorgung ist das „Internet der Dinge“ auf dem Vormarsch (vgl. Gabriel et al 2010).

Funketiketten als Wegbereiter

***RFID*-Funketiketten**[134] (auch „Tags“ oder „Transponder“) ermöglichen das automatische und berührungslose Identifizieren und Lokalisieren von Objekten und ersetzen damit immer mehr ältere Technologien wie Magnetstreifenkarten oder Barcodes. Auf den Etiketten können nicht nur Identifikations-Codes, sondern auch weitere Informationen bis hin zu Fingerabdrücken oder Fotos gespeichert sein. Der Einsatz von *RFID*-Etiketten bei Produkten von **Textilien** bis zu **Medikamenten** sowie in **Ausweisen und Karten** wie Reisepässen, Personalausweisen, Krankenkassenkarten oder Bürgerkarten hat bereits für viele Debatten in Bezug auf Privatsphäre gesorgt. Es wird befürchtet, dass sich durch die nicht wahrnehmbaren Auslesevorgänge bei mit *RFID*-Etiketten versehenen Waren, Kundenkarten oder Ausweisen negative Implikationen auf die informationelle Selbstbestimmung der BürgerInnen ergeben könnten (vgl. Sterbik-Lamina 2009).

Vernetzte Sensoren

Im *Internet der Dinge* sind *RFID*-Etiketten aber nur ein kleiner Teilbereich einer großen Palette an Technologien, die heute immer mehr Objekte mit ihrer Umgebung digital vernetzen. Die **drahtlose Kommunikation** bleibt dabei aber eine zentrale Komponente – von Mobilfunk-Technologien wie *GSM* oder *UMTS* über *Bluetooth* bis *WLAN* (vgl. Mattern 2005). Als Weiterentwicklung von RFID-Technologie spielt diesbezüglich auch der *NFC-Standard*[135] eine Rolle, der bisher hauptsächlich bei der bargeldlosen Zahlung kleiner Beträge zum Einsatz kommt. Ein weiterer wichtiger Aspekt ist die **Lokalisierbarkeit** von Objekten durch Technologien wie *GPS*-Ortung. Dazu spielt generell die Weiterentwicklung der Sensor-Technologie eine wichtige Rolle. Mit **Sensoren** werden die Daten aus Umgebung und Umwelt erfasst, gesammelt und für die Weiterverarbeitung nutzbar gemacht (vgl. Mattern 2005) – oft in Echtzeit. Durch die Integration von kleinen vernetzten Computern mit vielfältigen Sensoren in Alltagsobjekte werden diese Computer allgegenwärtig, dieser Trend wird auch unter dem Begriff **Ubiquitous Computing** diskutiert. Nach Mark Weiser (1991) werden die Computer dabei zunehmend unsichtbar – wie die „Kabel in der Wand“.

…von Körper und Haushalt bis Stadt und Arbeit

Auch Geräte wie *Smartphones* oder *Wearables* wie *Fitness-Tracker* oder *Smartwatches* werden im Kontext des *Internet der Dinge* diskutiert, die Entwicklung geht aber weit darüber hinaus. Der

133 Ashton, Kevin (2009): That 'Internet of Things' Thing. In the real world, things matter more than ideas. In: RFID Journal, 22.06.2009. Abgerufen am 20.09.2014 von http://www.rfidjournal.com/articles/view?4986

134 RFID (engl. „radio-frequency identification“): Passive Etiketten werden vom Lesegerät durch magnetische Wechselfelder oder hochfrequente Radiowellen mit Energie versorgt und können nur aus geringen Distanz von wenigen Zentimetern bis zu wenigen Metern ausgelesen werden. Mit aktiven RFID-Etiketten mit eigener Energieversorgung lassen sich höhere Reichweiten bis zu 10 Metern erreichen. Siehe auch: http://de.wikipedia.org/wiki/RFID

135 NFC (engl. „near field communication): http://de.wikipedia.org/wiki/Near_Field_Communication

jüngste Forschungsbericht des renommierten *Pew Research Center Internet Project* (2014) zählt beispielsweise folgende Felder und zukünftigen Anwendungsbereiche auf:

- **Körper und Gesundheit:** Verschiedenste Chips, tragbare oder eingebaute Geräte, die Aktivitäten, Gesundheit oder Fitness überwachen – und auch an Gesundheitsdienstleister übertragen. Außerdem werden auch andere überwacht – wie beispielsweise Kinder oder ArbeitnehmerInnen -, die entweder Geräte mit Sensoren bei sich tragen oder sich an Orten bewegen, die mit Sensoren ausgestattet sind. Sensorbrillen wie *Google Glass* werden unauffälliger.
- **Haushalt:** Alles ist fernbedienbar und mit vernetzten Sensoren ausgestattet – von Heizung, Kühlung, Gartenwässerung bis zu vernetzten Kühlschränken, Backöfen, Kaffeemaschinen, Badewannen, Rohrbruch- oder Feuermeldern.
- **Stadt und Infrastruktur:** Allgegenwärtige Sensoren auf Straßen, in Gebäuden oder Brücken zur Erfassung von Abnützung oder zur Regelung des Verkehrs – eventuell ergänzt durch *Apps*, die individuelle Verhaltensweisen mit dem Verkehr „synchronisieren" (Ernährung, Arbeitszeiten, Kalender). Weitere Beispiele: Sich selbst regelnde Stromnetze; Papierspender, die ein Signal geben, wenn sie leer sind; Mülleimer, die ein Signal geben, wenn sie voll sind.
- **Produktion und Handel:** Viele Objekte in Fabriken und Versorgungsketten sind mit Sensoren ausgestattet.

Gesellschaftliche Implikationen

Viele der 1.606 für die Studie interviewten ExpertInnen erwarten, dass **Anreize zur Verhaltensänderung** zum zentralen Treiber für das *Internet der Dinge* werden – beispielsweise zum Kauf eines Produkts oder zur Anregung von gesünderen oder sichereren Lebensweisen, bestimmten Arbeitsweisen oder der effizienteren Nutzung öffentlicher Güter. Diese Entwicklung würde „substanzielle Fragen" in Bezug auf die **Privatsphäre** aufwerfen – und auf die Möglichkeit der Menschen, „ihr eigenes Leben zu kontrollieren". Wenn alle Alltagsaktivitäten überwacht werden, würde das Ausmaß von *Profiling* und *Targeting* weiter wachsen und „soziale, ökonomische und politische Kämpfe verstärken".[136] Einige der befragten ExpertInnen warnen auch vor **negativen sozialen Folgen** durch automatisierte Feedbackschleifen und durch andere Algorithmen, die unangemessene Entscheidungen treffen könnten – oder vor der **Fehleranfälligkeit** komplexer Netzwerke, deren Wartung und Weiterentwicklung zu schwierig sein könnte. Nicht zuletzt wird eine neue **digitale Spaltung** prognostiziert – in Bezug auf diejenigen, die nicht „connected" sind, oder die nicht „connected" sein wollen.

Lösungsansätze

Andererseits könnte Internet-Technologie mit ihrer traditionellen Ende-zu-Ende-Architektur gleichzeitig auch die Lösung für manche dieser Risiken bereithalten – und die Menschen dazu ermächtigen, ihre Privatsphäre zu schützen. Mit **dezentralen „eigenen Clouds"**, die sowohl technische Intelligenz als auch Daten autonom verwalten und sich nur mit erwünschten Objekten, Services und Unternehmen vernetzen, könnte eine „People's Cloud of Things" genauso „persönlich und privat sein wie das eigene Haus". Der in der Studie zitierte Experte Doc Searls – Journalist und Mitarbeiter des *Berkman Center for Internet and Society* in Harvard - hofft, dass bei einem derartigen Ansatz auf den permanenten Datenfluss in Richtung zentralisierter Services und Unternehmen verzichtet werden könnte, die NutzerInnen mehr **Kontrolle über ihre persönlichen Daten** ausüben könnten und sieht trotzdem mögliche Geschäftsmodelle für Un-

136 Übersetzung durch den Verfasser, im Original: „The realities of this data-drenched world raise substantial concerns about privacy and people's abilities to control their own lives. If everyday activities are monitored and people are generating informational outputs, the level of profiling and targeting will grow and amplify social, economic, and political struggles."

ternehmen. Ansätze wie dieser werden unter dem Begriff ***Privacy by Design***[137] erforscht.

4.4.1. Von vernetzten Thermostaten über E-Book-Reader bis zur elektronischen Fußfessel für Babys

Geräte und Services zur Überwachung von Aktivitäten, Körper und Gesundheit zählen zu den relevantesten und gleichzeitig gesellschaftlich riskantesten Bereichen im Kontext des *Internet der* Dinge. Einige Beispiele für bereits erhältliche oder aktuell entwickelte Geräte und Anwendungen:

Vernetzte Objekte - von etabliert bis skurril

- **Vernetzte Thermostaten und Brandmelder:** Der 2014 von *Google* für 3,2 Milliarden Dollar übernommene [138] Hersteller *Nest Labs* [139] produziert ein Raumthermostat mit WLAN-Funkschnittstelle und Temperatur-, Feuchtigkeits-, Bewegungs- und Umgebungslichtsensoren, das in Kombination mit einer zentralisierten *App* das Alltagsverhalten der BewohnerInnen überwacht und die Raumtemperatur entsprechend regelt. Zusätzlich wird ein WLAN-Rauchmelder mit mehrere Sensoren für Rauch, Kohlenmonoxid, Hitze, Umgebungslicht und Bewegung angeboten.
- **Smart Meter**[140]**:** Intelligente Zähler messen den Verbrauch von Strom, Gas, Fernwärme oder Wasser und melden das Verbrauchsverhalten an den Versorger. Im 3. EU-Binnenmarktpaket von 2009[141] fordern europäisches Parlament und europäischer Rat, dass bis 2020 „mindestens 80% der Verbraucher bis 2020 mit intelligenten Messsystemen ausgestattet“ werden sollen.
- **E-Book-Reader:** Viele Geräte übertragen detaillierte Informationen zum Leseverhalten an Unternehmen, beispielsweise welche Bücher und welche Passagen darin wie oft, wie schnell und zu welchen Tageszeiten gelesen wurden (vgl. Alter 2012). Dies ermöglicht nicht nur weitgehende Aussagen über die LeserInnen, sondern könnte durch die detaillierten statistischen Auswertungsmöglichkeiten auch darauf Einfluss haben, wie Bücher in Zukunft geschrieben werden.
- **Vernetzte Fernseher:** Viele aktuellen TV-Geräte übertragen nicht nur Informationen zu besuchten Webseiten und teils Standort-Daten an die Hersteller, sondern auch Informationen über Fernsehgewohnheiten und angesehene Filme142.
- **Biometrische Kopfhörer:** Ein von der Firma *SMS Audio* in Kooperation mit *Intel* entwickelter Kopfhörer *BioSport*[143] misst mit einem optischen Sensor den Puls und zeichnet mit anderen Sensoren die Schrittzahl und die Höhe auf. Das deutsche Unternehmen *Bragi* arbei-

---

137 http://en.wikipedia.org/wiki/Privacy_by_Design

138 Sokolov, Daniel (2014): Google kauft Heimvernetzer Nest für 3,2 Milliarden Dollar. heise online, 14.01.2014. Abgerufen am 27.09.2014 von http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google/fuer-ueber-drei-milliarden-dollar-google-kauft-rauchmelder-firma-nest-12750875.html

139 https://nest.com (Abgerufen am 27.09.2014)

140 http://de.wikipedia.org/wiki/Intelligenter_Z%C3%A4hler

141 Richtlinie (EG) 2009/72 des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie (EG) 2003/54. Abgerufen am 27.09.2014 von http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:211:0055:0093:de:PDF

142 Laughlin, Andrew (2014): Smart TV spying – are you watching TV, or is it watching you? Which? Magazine, 20.08.2014. Abgerufen am 20.09.2014 von: http://blogs.which.co.uk/technology/tvs/smart-tv-spying-weve-investigated

143 Intel (2014): Biometric Headphones Will Optimize Workouts for Ultra-marathoners, Aspirational Exercisers and Everyone in Between. Pressemeldung, 14.08.2014. Abgerufen am 27.09.2014 von http://newsroom.intel.com/community/intel_newsroom/blog/2014/08/14/intel-and-sms-audio-to-supercharge-fitness-wearables

tet an Kopfhörern, die zusätzlich die Sauerstoffsättigung im Blut messen sollen.[144]

- **Intelligente Zahnbürste:** Das Unternehmen *Procter & Gamble* bietet mit seiner elektrischen Zahnbürste *Oral B Pro 7000*[145] ein Gerät an, das die Zahnputzaktivitäten via *Bluetooth* auf das *Smartphone* überträgt. Mit einer *App* können individuelle Putzprogramme und Ziele eingestellt und das Putzverhalten ausgewertet werden.
- **Vernetzter Ring:** Das Unternehmen *Logbar* arbeitet an einem am Finger zu platzierenden Ring mit Batterie, Touch-Bedienung, LED-Anzeige und Bewegungssensoren, der Daten via Bluetooth an andere Geräte oder Apps übertragen kann.[146]
- **Elektronische Tattoos:** Ein US-Forscherteam hat Gesundheitssensoren entwickelt, die sich wie entfernbare Tattoos auf die Haut drucken lassen und drahtlos mit Strom versorgt werden. Der Prototyp hält bis zu zwei Wochen und misst dabei Temperatur, ausgeübte Kräfte und Feuchtigkeitsstatus.[147] Das Produkt soll vom Unternehmen *mc10*[148] vermarket werden, das seine Produkte u.a. für Sport, Wellness, Kosmetik, Medizin, Baby-Überwachung und Militär anbietet. Auch *Motorola* hat ein Patent für ein elektronisches Tattoo angemeldet[149] - 2013 noch Teil von *Google*.
- **Socken, T-Shirts und Büstenhalter mit Sensoren:** Das Unternehmen *Sensoria* bietet Socken an, mit denen nicht nur Schrittzahl und Geschwindigkeit ausgewertet können, sondern auch, wie jemand beim Laufen auftritt und den Fuß abrollt. Die gemessenen Daten werden via Bluetooth an eine *Smartphone-App* übertragen. Außerdem werden T-Shirts und Büstenhalter angeboten, die den Puls messen.[150]
- **Intelligente Gabel:** Das Produkt *HAPIfork*[151] überwacht als „Smart Fork" bzw. „intelligente Gabel" die Anzahl der Gabelnutzungen pro Minute und pro Mahlzeit, die Dauer jeder Nutzung und die Gesamtdauer der Mahlzeiten. Die Daten werden via *Bluetooth* oder *USB* an eine *App* übertragen, die dabei helfen soll, gesünder zu leben, langsamer zu essen und durch die richtigen Zeitpunkte und Geschwindigkeiten von Mahlzeiten Gewicht zu verlieren.
- **Überwachung der Atmung:** *Spire* ist ein kleines tragbares Gerät, das eng am Körper getragen wird und sowohl Schritte als auch Atemmuster überwacht. Mit der zugehörigen *App* können aus den gemessenen Daten laut Hersteller etwa nicht nur die Dauer des Sitzens, Stehens oder Liegens ausgewertet werden, sondern durch die Analyse der Atemmuster auch psychische Belastung, Stress-Niveau oder Stimmung.[152]
- **Datenbrillen:** Brillen wie *Google Glass*[153] besitzen eingebaute Miniaturcomputer, Funkschnittstellen auf Basis von *Bluetooth* und *WLAN* sowie Sensoren wie Mikrofon, Digitalkamera, Beschleunigungssensor und GPS. Mit Hilfe des ins Sichtfeld eingeblendeten Bilds

144 Bragi (2014): The Dash. Wireless Smart In Ear Headphones. Spendenkampagne auf der Crowdfunding-Plattform Kickstarter. Abgerufen am 27.09.2014 von https://www.kickstarter.com/projects/hellobragi/the-dash-wireless-smart-in-ear-headphones

145 http://www.oralb-blendamed.de/de-DE/zahnpflege-produkte/oral-b-black-pro-7000-smartseries-elektrische-zahnbuerste (Abgerufen am 27.09.2014)

146 Logbar (2014): Ring. Shortcut Everything. Spendenkampagne auf der Crowdfunding-Plattform Kickstarter. Abgerufen am 27.09.2014 von https://www.kickstarter.com/projects/1761670738/ring-shortcut-everything

147 Orcutt, Mike (2013): Electronic Sensors Printed Directly on the Skin. MIT Technology Review, 11.03.2013. Abgerufen am 27.09.2014 von http://www.technologyreview.com/news/512061/electronic-sensors-printed-directly-on-the-skin/

148 http://www.mc10inc.com (Abgerufen am 27.09.2014)

149 Motorola Mobility LLC (2013): Coupling an electronic skin tattoo to a mobile communication device, US 20130297301 A1. Abgerufen am 27.09.2014 von http://www.google.com/patents/US20130297301

150 http://www.sensoriafitness.com (Abgerufen am 27.09.2014)

151 http://www.hapi.com/product/hapifork (Abgerufen am 27.09.2014)

152 https://spire.io (Abgerufen am 27.09.2014)

153 http://de.wikipedia.org/wiki/Google_Glass

können im Sinne von „Augmented Reality“[154] digitale Informationen über die Umwelt eingeblendet werden. Dazu muss das Gerät in der Lage sein, Objekte, Personen und deren Verhalten zu erkennen und daraus Schlüsse zu ziehen.

- **Intelligente Kleidung und „elektronische Fußfesseln“ für Babys:** Der Hersteller *Owlet Baby Care* bietet eine Fußmanschette an, die Puls und Atmung von Kindern überwacht und via Bluetooth an eine *App* überträgt. Der „Baby Monitor“ der Firma *Mimo* ist im Strampelanzug eingebaut, dient als *Babyfon* und vermisst Schlaf, Atmung, Aktivität, Position und Hauttemperatur.
- **Ortung von Handelsangestellten:** Das System *Theatro* besteht aus kleinen tragbaren Geräten für Handelsangestellte und einer Auswertungs-Software. Das System ermöglicht filialübergreifende Sprachkommunikation, die Ortung von Angestellten und bietet Auswertungsmöglichkeiten über deren Verhalten, Produktivität, Bewegungsmuster und über die Dynamiken im Team.[155]

154 http://de.wikipedia.org/wiki/Erweiterte_Realit%C3%A4t
155 http://theatro.com (Abgerufen am 27.09.2014)

5 Das Geschäft mit den persönlichen Daten

"The power of personal information lies at the heart of surveillance"
Neil M. Richards (2013), Harvard Law Review

Sowohl im deutschen Sprachraum als auch international existiert eine Vielzahl von Unternehmen, die sich in der einen oder anderen Weise dem Handel mit persönlichen Daten verschrieben haben. Im folgenden Kapitel soll anhand von Beispielen ein Überblick über Angebot und Praktiken dieser Unternehmen gegeben werden – vom **deutschen Sprachraum** über **internationale Player** bis zu neuen Entwicklungen im Feld von **Online-Tracking und Werbenetzwerken**.

5.1. Adresshandel und Listbroking im deutschen Sprachraum

Der An- und Verkauf von Postanschriften potenzieller KundInnen hat eine jahrzehntelange Geschichte und wird meist unter dem Begriff **Adresshandel**[156] gefasst. Als Teil des Direkt- bzw. Dialogmarketings nutzen viele Unternehmen nach verschiedenen Kriterien zusammengestellte und gefilterte Listen von Namen und Adressen für den Versand von personalisierten Angeboten und Werbung. Sind diese Adressen mit Zusatzinformationen wie Geschlecht, Alter, Einkommen, Bildung oder Hobbys angereichert, kann die Werbung besser auf die **Zielgruppen** abgestimmt werden. Dadurch können die EmpfängerInnen gezielter angesprochen werden und es erhöht sich die Wahrscheinlichkeit, dass die potenziellen KundInnen positiv reagieren – also beispielsweise eine Bestellung tätigen, ein bestimmtes Geschäft aufsuchen, sich für ein bestimmtes Produkt entscheiden oder einfach nur in Kontakt treten. Die erfolgreichen Reaktionen auf eine derartige Maßnahme wird als Rücklauf oder *Response*[157] bezeichnet und soll aus Unternehmenssicht möglichst hoch sein.

Marktführer und Marktvolumen

Unternehmen im Bereich Adresshandel decken insbesondere auch die Aufbereitung, Anreicherung, Verifizierung und Optimierung der dafür benötigten Adressbestände ab, diese Vorgänge werden als **Adressveredelung** bezeichnet. In ähnlicher Weise werden auch andere Kanäle wie Telefon oder E-Mail genutzt. Laut Deutscher Post gaben Unternehmen in Deutschland 2011 etwa 9,5 Mrd. Euro für voll adressierte Werbesendungen aus, für aktives Telefonmarketing und E-Mail-Marketing jeweils 2 Mrd. Euro[158]. Die Adressen werden über Adresshändler bzw. **Listbroker**[159] entweder für die einmalige oder für eine zeitlich uneingeschränkte Nutzung eingekauft. Das deutsche Bundeskartellamt schätzt das Marktvolumen für Adresshandel und -veredelung im Jahr 2004 auf etwa 770 Millionen Euro[160], der Markt wird von den Unternehmen ***ABIS** GmbH*, ***Acxiom** Deutschland GmbH*, ***AZ Direkt** GmbH*, ***Deutsche Post** Direkt GmbH*, ***EOS** Holding GmbH* und der ***Schober** Information Group Deutschland GmbH* dominiert.

Tochterfirmen und Kooperationen

EOS ist eine hundertprozentige Tochter des Versandhandelskonzerns ***Otto** Group*, *AZ Direkt*

156 http://de.wikipedia.org/wiki/Adresshandel
157 http://de.wikipedia.org/wiki/Response_(Marketing)
158 Deutsche Post (2012): Dialogmarketing in Deutschland 2012. Studie 24. Abgerufen am 09.07.2014 von https://www.bvdp.de/fileadmin/files/files/5_120619-Dialog_Marketing_Monitor_2012.pdf
159 http://de.wikipedia.org/wiki/Listbroker
160 Bundeskartellamt: Verfügung Fusionsverfahren Bertelsmann / InFoScore , 19.05.2005. Abgerufen am 09.07.2014 von http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Fusionskontrolle/2005/B9-32-05.pdf

Teil der *arvato AG*[161] - einer hundertprozentigen Tochtergesellschaft der ***Bertelsmann*** *Gruppe. ABIS* gehört zur ***Deutsche Post*** *Adress GmbH & Co. KG* - einem Gemeinschaftsunternehmen der *Deutschen Post DHL* und wiederum *Bertelsmann*. Darüber hinaus gibt es weitere Kooperationen – beispielsweise lizensierte[162] die *Deutsche Post Direkt GmbH* 2012 ihren gesamten Bestand von 37 Millionen Adressen an die *Schober Information Group*. Marktführer im Bereich der Aktualisierung von **Umzugsadressen** ist die *Deutsche Post Adress GmbH & Co. KG*, die die Daten aus dem Nachsendeservice der Deutschen Post vermarktet[163].

Woher stammen die Daten?

Die gehandelten Adressen werden von derartigen Unternehmen teilweise selbst zusammengestellt – beispielsweise durch Umfragen oder aus **öffentlich zugänglichen Verzeichnissen** wie Telefonbüchern, Vereins- und Firmenregistern. Außerdem werden Daten von anderen Unternehmen **zugekauft** - etwa aus Kundendatenbanken von Versandhändlern und Verlagen oder anderen Quellen.

5.1.1. Beispiel: AZ Direkt

Einer der größten deutschen Anbieter im Bereich Adresshandel ist *AZ Direkt*, ein Tochterunternehmen der *arvato AG*, die wiederum im Eigentum von *Bertelsmann* steht. *AZ Direkt* bietet laut Eigenangabe[164] mehr als **2.500 verschiedene Listen von KundInnen und InteressentInnen** anderer deutscher Unternehmen an, die nach weiteren Kriterien wie etwa letztes Kaufdatum, Postleitzahl, Geschlecht oder Produktgruppe „selektiert" werden können. In einem online verfügbaren Katalog[165] werden aktuell etwa Listen von 510.000 „aktiven Kunden" des ***RTL Club***, 374.900 „aktuelle Leser und ehemalige Abonnenten" der Wochenzeitung ***Die Zeit*** (vgl. Abb. 3) oder 2.155.000 Adressen einer „Werbedatei einer großen Tageszeitung" angeboten. Letztere umfasst laut Katalog einen „anspruchsvollen Personenkreis mit überdurchschnittlicher Schulbildung sowie entsprechender beruflicher und sozialer Stellung".

Von seriösen Zeitungen bis Erotikversand…

Dazu werden im Katalog mehrere in Segmente unterteilte Kundenlisten der Firmen *Yves Rocher* oder 270.200 „aktive Käufer" der *Versa Distanzhandel GmbH* angeboten, die in KäuferInnen der letzten 6, 12 und 24 Monate unterteilt ist. *Versa* ist Inhaber der Erotikversand-Marke ***Beate Uhse***, das Angebot wird im Katalog beworben als „überaus response-starke Adressen - immer wieder sehr erfolgreich eingesetzt in den Bereichen Glücksspiel, Versandhandel, Bank- und Versicherungsbranche, aber auch von Non-Profit-Organisationen". Adressen der letzten sechs Monate kosten € 150 pro Tausend, über ein Jahr alte Adressen nur € 140 pro Tausend, Mindestabnahmemenge sind 5.000 Adressen. Die Liste enthält 54% Männer und 46% Frauen, kann nach Geschlecht und Alter selektiert und „überschneidungsfrei nachgeliefert" werden.

---

161 http://de.wikipedia.org/wiki/Arvato

162 http://www.schober.de/unternehmen/zu-presse/mitteilungen-detail/news/440.html (Abgerufen am 09.07.2014)

163 http://www.deutschepost.de/de/p/postadress/kompetenzen/adressaktualisierung/move-umzugsdatenbank.html (Abgerufen am 09.07.2014)

164 http://www.az-direct.com/site/neukundengewinnung/kanaele-und-reichweiten/listbroking (Abgerufen am 09.07.2014)

165 AZ Direkt: Adressen für jede Zielgruppe. Listbroking. Abgerufen am 09.07.2014 von: http://www.az-direct.com/site/blaetterkatalog/listinfos

Kirchliche Verlage, Ökos und „passive Ältere“

Aber auch Adresslisten von **kirchlichen Verlagen und Zeitschriften** sind laut Katalog erhältlich, etwa Daten über 49.400 AbonnentInnen der katholischen Wochenzeitung „Tag des Herrn“ - herausgegeben von den katholischen Diözesen Mitteldeutschland. Laut Angebot sind die enthaltenen Personen zu 80% über 50 Jahre alt, „primär wertorientiert“ und kosten € 170 pro Tausend Adressen. Für eine Liste von 215.500 GewinnspielteilnehmerInnen „Drogerieartikel“ mit der „Einsatzempfehlung: Kosmetik- Schönheitsprodukte, Schmuck, Neuheiten und Reisen“ fallen nur € 150 pro Tausend an. Außerdem werden beispielsweise Kundenlisten wie 161.900 „**ökologiebewusste Personen**“, 178.200 „**Postkäufer von modischen Schuhen**“, 65.700 „**spendenaffine Akademiker**“, 3.051.100 „**passive Ältere**“, 3.466.900 „**kulturell Aktive**“ oder 460.700 **Lehrer** angeboten – letztere unterteilt in Hochschul-, Berufsschul-, Gymnasial-, Gesamtschul-, Realschul-, Hauptschul- und Grundschullehrer.

ListInfo

arvato
AZ DIRECT

Die Zeit

Potenziale

Bestell-Nr.: 1548200

Menge ca.	Selektion		Preis p. Tsd.
374.900	akuelle Leser und ehem. Abonn.	€	160,00
55.900	Shopkäufer und Buchserienkäufer	€	210,00

Zusatzinformationen

Männer	46 %
Frauen	54 %
Firma	
Echtaltersselektion	Nein
Durchschnittsalter	25-65 Jahre
Vornamenanalyse	Ja
Beilagen	Nein

Konditionen

Selektionskosten	€ 9,00 p.Tsd. mind. € 150,00
Zusatzselektionskosten	€ 9,00 p.Tsd.
Versandkosten	€ 35,00
Mindestabrechnung	70 %
Mindestabnahmemenge	10.000
Altersselektion	€ 9,00 p.Tsd.
überschneidungsfrei festhalten	mind. € 75,00
überschneidungsfrei nachliefern	

Sonstiges / Bemerkungen

Im Sinne der Transparenzpflichten nach dem BDSG (Novelle II) muss bei Nutzung der personenbezogenen Daten für schriftliche Werbung die Verantwortliche Stelle angegeben werden. Im Ausnahmefall der Spendenwerbung für steuerbegünstigte, gemeinnützige oder kirchliche Organisationen ist die Angabe der verantwortlichen Stelle nicht erforderlich.

DIE ZEIT wurde 1946 gegründet und zählt heute zu Deutschlands größten, überregionalen Wochenzeitungen. Die Qualitätszeitung bietet eine große Themenvielfalt: Fundierte Hintergrundberichte über Politik und Wirtschaft sind zentrale Bestandteile. Aber auch andere Themen, die unsere Gesellschaft bewegen, finden ausreichend Platz: Kultur und Wissenschaft, Technik und Medizin, Gesellschaft und Bildung, Reisen, Lifestyle, Autos und Sport. Der hohe redaktionelle Anspruch macht DIE ZEIT zu dem führenden Medium als Meinungsbildner und Multiplikator und ist damit das Leitmedium gehobener Zielgruppen.

Die Zielgruppe ist zwischen 25 und 65 Jahren alt. Tendenziell ist in den letzten Jahren ein Zuwachs an jüngeren Abonnenten zu beobachten.

Die Zielgruppe zeichnet sich durch einen überdurchschnittlich hohen sozialen Status und einen überdurchschnittlich hohen Bildungsgrad aus und lebt überwiegend in guten Wohngegenden.

Neben einem ausgeprägten Interesse an Politik und Wirtschaft gehören Themen wie Kunst, Sprachen und Weiterbildung zur Vorliebe der Zeit-Abonnenten / Shop- und Editionskäufern. Ebenso ist eine große Präferenz für Außer-Haus-Aktivitäten (Theater, Kino, Weiterbildung, Reisen etc.) vorhanden. Durch ihr hohes Einkommen besitzen sie eine überdurchschnittlich hohe Kaufkraft für exklusive Markenprodukte und eignen sich insbesondere für die Ansprache rund um die Themen Lifestyle, Geldanlagen und Kreditkarten. Als kritische Verbraucher legen sie Wert auf Qualität und achten auf gesundheitsbewusste und ökologische Aspekte.

Abbildung 3: *Angebotene Adressen der Wochenzeitung „Die Zeit“. Quelle: AZ Direkt Blätterkatalog.*

Potenzielle SpenderInnen

In der im Online-Katalog angeführten Liste „AZ Zielgruppen Spender“ werden 5.311.200 Adressen von potenziellen „Spendern“ angeboten, unterteilt in die Kategorien **Behindertenhilfe**, **Entwicklungshilfe**, **Sofort-/Nothilfe**, **Kirche/Glaubensgemeinschaften**, **Umweltschutz**, **Wohlfahrtspflege**, **Kinderhilfe**, **Tierschutz**. Bei der Generierung der Liste wurden laut Angebot „neben zahlreichen Marketingdaten wie Alter und Kaufkraft, Konsumneigung und Wohnumfeld“

auch „Spender-Profile“ wie „sozial“, „religiös“, „kulturell“ oder „traditionell“ berücksichtigt. Dabei wurde laut Eigenangabe „psychografische Adress-Selektion auf der Grundlage semiometrischer Werte-Steckbriefe aus anonymen TNS infratest Marktforschungs-Ergebnissen“ eingesetzt. Eine **Selektion nach Alter** ist möglich.

30 Millionen Profile

Darüber hinaus bietet *AZ Direkt* als „Ergänzung zum Listbroking“ mit dem Produkt *Audience Targeting System AZ DIAS* „ca. **30 Millionen Adressen**“ an, die für „volladressierte Werbung genutzt werden können“[166]. Für „gezielte Adressselektionen“ stünden dabei „mehr als **600 adressqualifizierende Profilinformationen** zum Beispiel zu Soziodemografie, Psychografie, Konsumeigenschaften, Lebensphasen u.v.m.“ zur Verfügung. Bei diesen „Consumer-Adressen“ sei AZ Direkt „Adresseigentümer“ und somit bestehe im Gegensatz zum Listbroking „kein Konkurrenzausschluss“.

Risikobereit oder sicherheitsorientiert?

Mit diesem Produkt könnten Unternehmen auch die Daten ihrer Bestandskunden analysieren und damit „fundierte Adressbewertungsmodelle (Marketing-Scorekarten) und Kunden- und damit Zielgruppenprofile“ entwickeln. Für die Neukundengewinnung werden wiederum segmentierte Listen zu verschiedenen „Interessenschwerpunkten“ angeboten. In folgender Tabelle finden sich einige dieser angebotenen Listen, die jeweils **mehrere 100.000 bis mehrere Millionen Personen** inklusive Postanschriften oder E-Mail-Adressen beinhalten[167]:

Interessenschwerpunkt	Bezeichnungen der Adresslisten bei AZ Direkt
Sport & Fitness	Sportbegeisterte, Naturfans
Gesundheit	Gesundheits-Fans, Wellness-Liebhaber, Kinderkrippe
Spielwaren & Babybedarf	Familien, Junge Familien
Wohnen & Garten	Hobbygärtner, Heimwerker, Möbel, Lohas, Dekorateure
Essen & Trinken	Feinschmecker, Hobbyköche, Lohas, Gesunde Esser
Nonfood-Konsumgüter	Tierliebhaber, Power-Shopper, Windelbar, Best Ager
Finanzen	Kreditkarte, Immobilien, Hypothekendarlehen, Ratenkredit, Vorsorger, Sparer, Erstes Gehalt
Versicherungen	Individualistisch-risikobereite, Sozial-sicherheitsorientierte, Job Starter, Best Ager, Familien

Tabelle 13: *Vom Unternehmen AZ Direkt angebotene Adresslisten. Quelle: AZ Direkt.*

Ethisch bedenklich?

Die von Unternehmen wie *AZ Direkt* angebotenen Daten ermöglichen potenziell **weitgehende Aussagen über die enthaltenen Personen** und deren Interessen, Vorlieben, Konsumverhalten, Lebenssituation, Lebensstil und ökonomischer Situation. Unter dem „Interessenschwerpunkt Finanzen“ werden etwa Daten über Menschen mit Hypothekendarlehen oder Ratenkrediten angeboten, unter dem Schwerpunkt „Versicherungen“ Daten über „individualistisch-risikobereite“ Menschen. Daten über **ältere Menschen**, **spendenwillige Personen** oder aus **Gewinnspielen** werden in einer Art und Weise beworben, die zumindest ethisch bedenklich erscheint. Ebenso erscheint es fragwürdig, wenn die Rede davon ist, dass Adressen etwa sehr erfolgreich im Bereich **Glücksspiel** eingesetzt würden.

Wissen die Betroffenen Bescheid?

Darüber hinaus stellt sich die Frage, ob etwa LeserInnen der Wochenzeitung *Die Zeit,* KundInnen von *Beate Uhse* oder von katholischen Verlagen und Versandhandelsunternehmen wirklich damit rechnen, dass ihre Daten auf diese Art und Weise verwertet werden. Es wäre daher interessant, zu untersuchen, wie viele der Betroffenen sich über diese Praktiken wirklich im Klaren

166 http://www.az-direct.com/site/neukundengewinnung/targeting-services/zielgruppenidentifizierung (Abgerufen am 09.07.2014)

167 http://www.az-direct.com/site/neukundengewinnung/targeting-services/az-target-groups (Abgerufen am 09.07.2014)

sind.

5.2. Negativlisten, Bonitätsbewertung und Scoring im deutschen Sprachraum

Adresshandel und -veredelung und Direktmarketing sind eng mit dem Sektor der **Wirtschaftsauskunfteien** und **Inkassoinstitute** verknüpft. Derartige Unternehmen sammeln Informationen zur Bewertung von Zahlungsmoral und Kreditwürdigkeit und stellen diese Informationen anderen Unternehmen zur Verfügung – früher hauptsächlich in Form von Negativlisten bzw. „schwarzen Listen". Heute kommen **komplexe Scoring-Modelle** zum Einsatz, die möglichst viele persönliche Lebensumstände und allgemeine statistische Informationen einbeziehen und daraus für jede erfasste Person einen Punktewert (Score) berechnen, der die Wahrscheinlichkeit eines Zahlungsausfalls angibt.

Unübersichtlicher Sektor

Wirtschaftsauskunfteien bieten unter anderem **Bonitätsprüfungen über Privatpersonen** an, der Sektor ist eng mit den Bereichen Adresshandel, Direktmarketing, Risikomanagement, Inkasso und Finanzdienstleistungen verknüpft. Die dominanten Unternehmen arbeiten meistens in mehreren dieser Bereiche – manche betreiben Kundenkarten-Systeme oder verwalten Daten für Versicherungen. Die Unternehmen und ihre unzähligen Tochterfirmen sind unübersichtlich miteinander verflochten. Abgesehen von Marketing-Aussagen existieren oft nur wenige zuverlässige Informationen über ihre Tätigkeiten und den Umgang mit den Daten von KonsumentInnen.

Diskriminierung durch intransparente Algorithmen?

In einer 2014 vom *Institut für Technikfolgenabschätzung* im Auftrag der *Bundesarbeitskammer* veröffentlichten Studie über „Credit Scoring in Österreich" wurden die rechtlichen Rahmenbedingungen und die zentralen Stakeholder der Branche in Österreich umfassend dargestellt, gefolgt von einer kritischen Auseinandersetzung mit den sozialen Implikationen des Scorings von Privatpersonen (vgl. Rothmann et al 2014). Dabei wurde unter anderem festgehalten, dass die eingesetzten Algorithmen **hochgradig intransparent** seien, die VerbraucherInnen schlecht über diese Methoden informiert seien und Scoring potenziell **fehleranfällig** sei. Den herangezogenen Daten mangle es oft an „Aktualität und unmittelbarem Bezug zum Zahlungsverhalten" und die eingesetzten quantitativ-statistischen Verfahren könnten die Vielschichtigkeit des Lebens niemals objektiv wiedergeben. So könne die „automationsgestützte Kreditwürdigkeitsbewertung letztlich zu wirtschaftlicher Ungleichbehandlung und stereotyper Diskriminierung führen".

Rechtliche Basis für „Scoring" in Deutschland ist der § 28b[168] des deutschen Bundesdatenschutzgesetzes, der es mit bestimmten Einschränkungen erlaubt, zum „Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses" einen „Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen" zu erheben und zu verwenden.

168 § 29 Dt. Bundesdatenschutzgesetz (BSDG): Scoring. Online: http://www.gesetze-im-internet.de/bdsg_1990/__28b.html

5.2.1.1. Beispiele: Schufa und Creditreform

Die bekannteste deutsche Wirtschaftsauskunftei ist die ***Schufa***[169], die laut Eigenangabe[170] Daten über **66,3 Millionen Privatpersonen** gespeichert hat. Als Ergänzung zu Basisdaten wie Name, Geschlecht, Geburtsdatum- und -ort, aktueller und früherer Anschriften erwirbt die *Schufa* regelmäßig Daten von Vertragspartnern – unter anderem über **Girokonten**, **Kreditkarten**, **Kredit- und Leasingverträge**, **Zahlungsstörungen**, **Telekommunikationskonten** oder **Kundenkonten beim Handel** (vgl. Korczak et al 2009). Die Daten werden mit „Angaben aus öffentlichen Verzeichnissen und amtlichen Bekanntmachungen" ergänzt (u.a. **Insolvenzverfahren**, **Zwangsvollstreckungen**). Neben einem Basis-Score werden daraus mehrere branchenspezifische Score-Werte berechnet.

Fehlerhafte, unvollständige oder falsche Einträge

Bei einer empirischen Studie im Auftrag des deutschen Bundesministeriums für Verbraucherschutz mit 100 Testpersonen wurde 2009 festgestellt, dass **45% der Eigenauskünfte** „fehlerhafte, unvollständige oder falsche Eintragungen" aufgewiesen hätten (vgl. Korczak et al 2009). Die Basis-Scores wären zwar „offenkundig mathematisch berechnet" worden, ihre „inhaltliche Bedeutung" aber erschiene „beliebig und willkürlich". Mit einem Gesamtumsatz von 123 Mio. Euro im Jahr 2013 gehört die *Schufa* im Bereich Scoring aber nur zu den mittelgroßen Anbietern.

Über 1.000 Merkmale

Die ***Creditreform AG*** – nach Eigenangabe die größte Wirtschaftsauskunftei Europas - deckt mit ihren Tochterfirmen und über 4.500 Angestellten mehrere Bereiche von Bonitätsbewertung und Scoring bis Direktmarketing ab. Darüber hinaus wird etwa vom Tochterunternehmen ***Microm***[171] eine Datenbank betrieben, bei der Konsumentenadressen mit „microgeographischen und über 1.000 soziodemographischen, sozioökonomischen und psychographischen Merkmalen**"** selektiert werden können[172]. Das Unternehmen bietet 36 Millionen Privatadressen in **Deutschland**, 3,2 Millionen in **Österreich** und 6 Millionen in der **Schweiz**.

5.2.2. Beispiel: arvato infoscore

Ein weiterer großer Anbieter von Wirtschaftsinformationen ist die *arvato infoscore GmbH*[173] - wie die zuvor erwähnte Firma *AZ Direkt* eine Tochterfirma der *arvato AG* und damit Teil von *Bertelsmann*. Das mit 6.000 Angestellten in 21 Ländern tätige Unternehmen hat laut Eigenangabe[174] „Negativinformationen" zu **7,8 Mio. Personen** gespeichert, bearbeitet jährlich **100 Mio. Bonitätsabfragen** und versendet **26 Mio. Inkassoschreiben** pro Jahr. Neben Bonitätsprüfungen, Adressverifizierungen werden unter dem Titel „Risikomanagement" viele weitere Dienstleistungen angeboten, deren genauer Charakter manchmal eher vage bleibt:

---

169 http://de.wikipedia.org/wiki/Schufa

170 https://www.schufa.de/de/private/unternehmen/zahlendatenfakten/zahlendatenfakten.jsp (Abgerufen am 09.07.2014)

171 http://www.microm-online.de (Abgerufen am 09.07.2014)

172 Microm Consumer: Adressen für ihre Neukundengewinnung. Abgerufen am 18.09.2014 von http://www.creditreform.de/Ressourcen/PDF/Downloads/Marketing_Services/Consumer_Marketing/Broschuere_microm_CONSUMER.pdf

173 http://www.arvato-infoscore.de (Abgerufen am 09.07.2014)

174 http://www.arvato-infoscore.de/de/unternehmen/daten-fakten (Abgerufen am 09.07.2014)

Nicht lukrative KundInnen meiden?

Durch das Angebot ***Antrags-Scoring***[175] können etwa offenbar NeukundInnen, die einen Kredit oder einen Kauf anstreben, vorab bewertet werden. Damit soll es möglich werden, „Kundengruppen mit hohen bzw. niedrigen Ertragschancen bei Antragstellung zu unterscheiden" - oder anders formuliert: „Kunden mit hohem Ertragspotenzial sollen gewonnen, Kunden mit hohem Risiko von Anfang an gemieden" werden. ***Storno-Scoring***[176] soll hingegen ermöglichen, die „Loyalität und damit die Stornowahrscheinlichkeit" zu prognostizieren und die „Kommunikationsstrategie" darauf anzupassen. ***Verhaltens-Scoring*** soll ein „einheitliches Risikomaß für das gesamte Portfolio" eines Unternehmens liefern, das „auf dem vergangenen Verhalten jedes Kunden basiert und eine zuverlässige Prognose für die Zukunft erlaubt"[177], damit „strategische Entscheidungen im Kräftefeld von Risikoabwägung, Portfolio-Rentabilität und Optimierung der Kundenbeziehungen gesteuert" [178] werden können.

Sämtliche Daten „verdichten und integrieren"

Mit dem von *arvato* ebenfalls angebotenen ***infoRate+ System***[179] könne zur „Bewertung eines Konsumenten auf vielfältigste Datenquellen zugegriffen" werden - unter anderem auch auf „Daten aus der AZ Direct-Adressdatenbank". Über das System ließen sich „sämtliche vorhandenen internen und externen Daten verdichten und integrieren". Auch Mikrogeografie-Analyse wird angeboten – also die Bewertung von Personen nach statistischen Informationen über Wohnort bzw. -bezirk[180]. Unter der Bezeichnung *Profile Tracking*[181] bietet *arvato* offenbar auch die **Identifikation von Online-NutzerInnen** anhand digitaler Fingerabdrücke ihrer Internetzugangsgeräte, was „deutlich bessere Ergebnisse als Cookie-basierte Systeme" liefern soll. Jedes Gerät – „ob PC, Tablet, Smartphone oder Spielkonsole" - hinterließe eine „eindeutige und identifizierbare Spur, die sogenannte Hash-ID." Mit seiner „herausragenden Tracking-Technologie" verfüge man „über die Fähigkeit, einzelne Internetzugangsgeräte anhand dieser Hash-ID eindeutig und in Echtzeit zu erkennen".

Kundenclubs und Anreizsysteme

Die *arvato AG* ist gleichzeitig ein großer deutscher Anbieter bei Betrieb und Umsetzung von Kundenbindungsprogrammen und betreibt „Kundenclubs, Kundenkartenprogramme, individuelle Prämienlösungen für Endkunden, Bonusprogramme für Geschäftspartner ebenso wie spezielle Promotionslösungen und andere individuelle Anreizsysteme"[182]. Zu den KundInnen von *arvato* zählt u.a. die Lufthansa und deren Programm ***Miles & More***[183]. Das Unternehmen betreibt über eine Tochterfirma außerdem die ***DeutschlandCard***[184], ein Kundenbindungsprogramm, das unter anderem mit *Edeka*, der *Deutschen Bank*, *L'TUR*, *Hertz*, *RWE*, *Schülerhilfe* und *Esso* kooperiert und dabei die Einkaufstransaktionen von vielen Millionen BürgerInnen verarbeitet.

Keine „schwarze Liste" über Versicherte

Außerdem betreibt[185] *arvato* über die Tochterfirma „Informa Insurance Risk and Fraud Preventi-

175 http://www.arvato-infoscore.de/dienstleistungen/risikomanagement/antrags-scoring (Abgerufen am 09.07.2014)
176 http://www.arvato-infoscore.de/dienstleistungen/risikomanagement/storno-scoring (Abgerufen am 09.07.2014)
177 http://www.arvato-infoscore.de/dienstleistungen/risikomanagement/verhaltens-scoring/effektives-instrument (Abgerufen am 09.07.2014)
178 http://www.arvato-infoscore.de/dienstleistungen/risikomanagement/verhaltens-scoring (Abgerufen am 09.07.2014)
179 http://www.arvato-infoscore.de/dienstleistungen/risikomanagement/inforate (Abgerufen am 09.07.2014)
180 http://www.arvato-infoscore.de/dienstleistungen/risikomanagement/inforate/online-kundenbewertung (Abgerufen am 09.07.2014)
181 http://www.arvato-infoscore.de/profile-tracking (Abgerufen am 09.07.2014)
182 http://www.arvato.com/de/leistungen/crm.html (Abgerufen am 09.07.2014)
183 http://www.arvato-systems.de/fileadmin/downloads/customer_solutions/CS_Lufthansa_Swimm_2011.pdf (Abgerufen am 09.07.2014)
184 http://de.wikipedia.org/wiki/DeutschlandCard
185 Marwede-Dengg, Claudia (2013): Versicherungen: Unter Verdacht. Euro am Sonntag, 07.09.2013. Abgerufen am 10.07.2014 von http://www.finanzen.net/nachricht/private-finanzen/Auskunftei-fuer-

on GmbH“[186] das ***Hinweis- und Informationssystem (HIS) der deutschen Versicherungswirtschaft***, das bestimmte Daten über Versicherte zentral verwaltet – etwa in den Sparten KFZ, Unfall, Rechtsschutz, Lebensversicherung, Berufsunfähigkeit, Pflegerente, Transport, Reiserücktritt oder Haftpflicht. Erfolgt bei einer teilnehmenden Versicherung ein Schadens- oder Leistungsfall, erfolgt eine Meldung an dieses System. 2007 wurden ca. **9,5 Millionen Meldungen** verwaltet[187]. Eine Meldung erfolgt laut Eigenangabe[188] beispielsweise in folgenden Fällen: Atypische Schadenhäufigkeiten, besondere Schadenfolgen, erschwerte Risiken, Auffälligkeiten im Schaden-/Leistungsfall. In der FAQ wird in Abrede gestellt, dass es sich dabei um eine „schwarze Liste“ handeln würde. Ein HIS-Eintrag wäre „für den Versicherer ein Signal, bestimmte Vorgänge in der Bearbeitung näher zu betrachten“, das System würde „den Erkenntnisprozess des Versicherers“ unterstützen.

Gesundheitssektor

Unter der Marke ***arvato Healthcare***[189] bietet eine weitere Tochterfirma darüber hinaus „Patienten- und Versichertenkommunikation“ – unter anderem „maßgeschneiderte Lösungen für Primärprävention, Bonusprogramme und die Betreuung von Patienten“[190], Maßnahmen zur Steigerung der „Kundenbindung“ oder „Präventionsprogramme“ für MitarbeiterInnen von Unternehmen oder Versicherte von Krankenkassen. Für Apotheken werden Bestellsysteme, Bestellannahme, Logistik, Rechnungsstellung und Reporting angeboten[191] – inklusive „Risk-Management“ bezüglich „Verschreibung“ und „Belieferung“. Alle „Patienten- und Kundendaten“ würden allerdings „gemäß der Datenschutzrichtlinien in einem speziell gesicherten Trust Center“ gespeichert[192].

Österreich

Das Unternehmen ist in Form der *infoscore austria GmbH*[193] auch in Österreich tätig und bietet unter anderem „Bonitätsprüfung (über Kooperationspartner)“, die Zusammenarbeit mit dem Mutterhaus *arvato Financial Solutions* sowie den „Zugang zu weiteren Geschäftsfeldern der *arvato AG*, wie z.B.: Adressmanagement.“

Welche Daten für welche Zwecke?

Die Eigendarstellung der in Deutschland, Österreich und vielen anderen Ländern tätige Bertelsmann-Tochterfirma *arvato* stellt in Aussicht, dass umfangreiche Daten über KonsumentInnen aus unterschiedlichsten Quellen zur Verfügung stünden und dass „sämtliche vorhandenen internen und externen Daten“ von Unternehmen „verdichtet und integriert“ werden könnten. Auf den vielen Websites von Mutter- und Tochterunternehmen mit teils redundanten Angeboten erscheint manchmal unklar, welche Datenbestände und Dienstleistungen welchen Branchen zu welchen Zwecken und unter welchen Regulierungen zur Verfügung gestellt werden.

Versicherer-Versicherungen-Unter-Verdacht-2630684

186 http://www.informa-irfp.de (Abgerufen am 09.07.2014)

187 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2007): Hinweis- und Informationssystem der Versicherungswirtschaft, 03.07.2007. Abgerufen am 10.07.2014 von https://www.datenschutzzentrum.de/wirtschaft/20070703-his.htm

188 http://www.informa-irfp.de/selbstauskunft-und-datenschutz/haeufige-fragen/7-welche-sachverhalte-fuehren-zu-einer-meldung-an-das-his/ (Abgerufen am 09.07.2014)

189 http://www.arvato-healthcare.de (Abgerufen am 20.09.2014)

190 http://www.arvato-healthcare.de/de/loesungen/patientenkommunikation.html (Abgerufen am 20.09.2014)

191 http://www.arvato-healthcare.de/de/loesungen/direct-to-pharmacy.html (Abgerufen am 20.09.2014)

192 http://www.arvato-healthcare.de/de/kompetenzen/it.html (Abgerufen am 20.09.2014)

193 https://www.arvato-infoscore.at (Abgerufen am 20.09.2014)

5.3. Datenhandel in den USA und international

In den USA existieren einige Unternehmen, die sowohl in Bezug auf Menge und Umfang der gesammelten persönlichen Daten als auch in Bezug auf die Art ihrer Verwertung weit über das hinausgehen, was Firmen in Österreich oder Deutschland anbieten. **Data Broker** (Datenhändler) oder *Information Resellers* sind laut dem *United States Government Accountability Office* Unternehmen, die Informationen aus vielen unterschiedlichen Quellen sammeln – inklusive persönlicher Informationen über KonsumentInnen – zum Zweck des Weiterverkaufs an andere Unternehmen oder an staatliche Behörden (vgl. GAO 2006).

Data Broker

Auch die Verknüpfung von Daten über KonsumentInnen mit **Echtzeit-Datenflüssen aus Netz** und *Social Media* ist in den USA schon weit fortgeschritten. Bis vor kurzem waren noch kaum Informationen über die Tätigkeiten dieser Firmen, die oft über **umfangreiche Dossiers** über die gesamte US-Bevölkerung und darüber hinaus verfügen, bekannt. Trotz geringer Affinität zu Datenschutz und dem nicht vorhandenen „Recht auf informationelle Selbstbestimmung" im europäischen Sinn gab es in den letzten Jahren aber immer mehr **mediale Berichterstattung** und eine **öffentliche Debatte** über die Praktiken dieser Unternehmen.

FTC-Bericht über 9 Unternehmen

Als vorläufiger Höhepunkt erschien im Mai 2014 ein Bericht der *Federal Trade Commission* (vgl. FTC 2014), in dem stellvertretend für die Branche der *Data Brokers* die neun Unternehmen ***Acxiom***, ***Corelogic***, ***Datalogix***, ***eBureau***, ***ID Analytics***, ***Intelius***, ***PeekYou***, ***Rapleaf***, ***Recorded Future*** untersucht wurden. Als Ergebnis wurde unter anderem festgestellt, dass *Data Brokers* Daten von KonsumentInnen „aus umfassenden Online- und Offline-Quellen" von Zahlungsverhalten über Aktivitäten in sozialen Medien, Zeitschriften-Abos bis zu religiösen und politischen Zugehörigkeiten sammeln – und das „**größtenteils ohne das Wissen der Konsumenten**"[194].

Enorme Mengen an Daten

Die Unternehmen hätten eine enorme Menge an Daten über beinahe alle US-Haushalte, deren kommerzielle Transaktionen sowie über einzelne KonsumentInnen gespeichert. Die *FTC* hat verschiedene Online- und Offline-Quellen dieser Unternehmen und die Wege, die die persönlichen Daten gehen, exemplarisch zusammengefasst:

KonsumentInnen…	Daten werden gesammelt und an *Data Broker* weitergegeben von:
veröffentlichen Informationen online	Data Brokers
kaufen Online	Online-Shops
registrieren sich auf Websites	Websites
kaufen in Geschäften	Geschäfte
füllen Garantiekarten aus	Unternehmen
kaufen Häuser	Lokale Regierungsbehörden

Tabelle 14: *Data Broker in den USA: Beispiele für deren Quellen und die Wege der persönlichen Daten. Quelle: FTC, 2014*

194 Übersetzung durch den Verfasser, im Original: „Data brokers collect consumer data from extensive online and offline sources, largely without consumers' knowledge" (FTC 2014)

Die neun untersuchten Unternehmen in den USA beziehen ihre Daten von Behörden sowie aus öffentlichen und kommerziellen Quellen. Einige Beispiele:

Behörden	Öffentliche Quellen	Kommerzielle Quellen
Professionelle Lizenzen, z.B. PilotInnen, ÄrztInnen, RechtsanwältInnen, ArchitektInnen	Telefonverzeichnisse und andere Verzeichnisse	Telekom-Unternehmen
Andere Lizenzen, z.B. Jagd, Fischerei	Medienberichte	Autohändler
Immobilieneigentum, z.B. Steuerakten, Wertabschätzungen, Pfandrechte, Urkunden, Hypotheken)	Öffentliche Online-Inhalte, z.B. von Websites, Blogs und Social Media (via Web-Crawler)	Einkaufs- und Zahlungsverhalten
Wählerverzeichnisse, z.B. Namen, Adressen, Geburtsdatum, Parteizugehörigkeit		Marketing-Umfragen, Garantiekarten, Gewinnspiele
Fahrzeugpapiere, Verkehrsstrafen		Online-Registrierungen, z.B. Websites in den Bereichen Handel, Nachrichten, Reise
Gerichtsakten, z.B. Strafregister, zivilrechtliche Prozesse und Urteile, Geburts-, Heirats-, Scheidungs- und Todesurkunden		

Tabelle 15: *Beispiele für Quellen, aus denen Data Broker in den USA persönliche Daten beziehen. Quelle: FTC, 2004*

Daten von Behörden spielen für *Data Broker* in den USA schon seit Jahrzehnten eine wichtige Rolle. Diese persönlichen Daten werden nicht immer direkt von den Behörden erworben, sondern teils von anderen Unternehmen gekauft - oder sogar durch Besuche bei lokalen Behörden manuell erfasst. Da es in den USA kein zentrales Melderegister gibt, sind die Daten aus **Wählerverzeichnissen** oder **Führerschein-Daten** eine bedeutende Quelle für verifizierte Basis-Informationen. Darüber hinaus sammeln die neun untersuchten *Data Broker* laut *FTC* detaillierte Transaktionsdaten über das Einkaufs- und Zahlungsverhalten von **190 Millionen Personen** – und von über **2.600 Handelsunternehmen**. Aus obiger Übersicht wird deutlich, welche gewaltige Steigerung der Datenqualität und –quantität durch die automatisierte Einbeziehung des schier unerschöpflichen Vorrats an öffentlichen und nicht-öffentlichen Online-Informationen möglich wird.

Heikle Schlussfolgerungen über KonsumentInnen

Data Brokers kombinieren, analysieren und segmentieren die gesammelten Daten und erstellen daraus Prognosemodelle. Laut *FTC* werden dabei teils heikle (englisch: „sensitive“) Schlussfolgerungen über einzelne Personen gemacht – etwa über **ethnische Zugehörigkeit**, **Einkommen**, **Gesundheit** oder **Elternschaft**. Einige *Data Brokers* speichern die gesammelten Daten unbefristet oder kombinieren Online- und Offline-Informationen, um Produkte online zu vermarkten.

Die gesammelten Daten werden oft über mehrere Unternehmen hinweg weitergegeben, allein sieben der neun Firmen haben bereits Daten mit mindestens einer anderen untersuchten Firma ausgetauscht. In Folge wäre es für die KonsumentInnen beinahe unmöglich, die Quelle der über sie gesammelten Informationen herauszufinden.

5.3.1. Beispiel: Datalogix, eBureau, PeekYou, Recorded Future, Lexis Nexis

Einige der von der *FTC* erwähnten *Data Broker*:

Partnerschaft mit Facebook

- ***Datalogix***[195] verfügt nach Eigenangabe etwa über Datensätze über beinahe jeden US-Haushalt und über mehr als eine Trillion Transaktionsdaten von KonsumentInnen. Im September 2012 hat *Datalogix* eine Partnerschaft mit *Facebook* bekanntgegeben, um zu vergleichen, wie oft eine Milliarde NutzerInnen Online-Werbung für Produkte auf *Facebook* sehen und den entsprechenden Kauf dann in einem Geschäft durchführen.
- ***eBureau***[196] stellt Prognosen, Scoring und Analyse-Services auf Basis persönlicher Daten zur Verfügung – unter anderem für die Bereiche Marketing, Finanzwirtschaft und Online-Handel. Neben Bonitätsprüfungen und Angeboten zur Unterstützung von Direktwerbung, dem Betrieb von Call Centern oder von *Customer Relationship Management* (CRM) werden Produkte angeboten, die die Wahrscheinlichkeit vorhersagen, ob Personen zu profitablen KundInnen werden – oder ob das Betrugsrisiko zu hoch ist. Laut Eigenangabe werden monatlich drei Milliarden Datensätze über KonsumentInnen gesammelt.

Auswertung von Websites und Social Media

- ***PeekYou***[197] analysiert laut Eigenangabe Inhalte von mehr als 60 „Social Media"-Seiten sowie von Websites und Blogs, identifiziert die beteiligten Personen und verbindet deren „verstreute digitalen Fußabdrücke in einen umfassendes Datensatz ihrer Online-Identität".
- ***Recorded Future***[198] zeichnet historische Daten über KonsumentInnen und Firmen im Netz auf und nutzt diese Informationen, um das zukünftige Verhalten von KonsumentInnen und Firmen vorherzusagen. Im Oktober 2014 hatte *Recorded Future* Zugriff auf Informationen von 596.132 verschiedenen Websites in sieben Sprachen. Auf der Website finden sich Angebote sowohl für Unternehmen als auch für Militär und Geheimdienste. Seit 2009 sind unter anderem *Google* und *In-Q-Tel* – und damit indirekt der US-Geheimdienst CIA – an der Firma finanziell beteiligt[199].

Ein weiterer großer Player…

Die in den USA vor etwa zehn Jahren immer wieder kontrovers diskutierte [200] Firma **Choicepoint**[201] mit umfangreichen Datensätzen über 220 Millionen Menschen wurde im Jahr 2008 von *Reed Elsevier* gekauft und ist nun Teil der Risikomanagement-Sparte von deren Tochterunternehmen ***Lexis Nexis***[202]. Das Unternehmen gibt an, Daten über 500 Millionen KonsumentInnen[203] zu besitzen, arbeitet laut Eigengabe für alle 50 der 50 größten US-Banken, für 70% der regionalen Regierungsbehörden, für 80% der US-Bundesbehörden[204] und bietet laut Website unter anderem „Risikomanagement-Lösungen" in den Bereichen Versicherung, Handel und für den Gesundheitssektor an.

Social Media und biometrische Daten

Angeboten werden unter anderem Daten über die **Kreditwürdigkeit** oder **Hintergrund-Überprüfungen von ArbeitnehmerInnen**, mit dem Service „Resident Data" können sich Immo-

195 http://en.wikipedia.org/wiki/Datalogix
196 http://www.ebureau.com (Abgerufen am 25.09.2014)
197 http://www.peekyou.com (Abgerufen am 25.09.2014)
198 http://en.wikipedia.org/wiki/Recorded_Future
199 Shachtman, Noah (2010): Exclusive: Google, CIA Invest in 'Future' of Web Monitoring. Wired, 28.07.2010. Abgerufen am 25.09.2014 von http://www.wired.com/2010/07/exclusive-google-cia/
200 O'Harrow, Robert (2005): They're Watching You. Bloomberg Businessweek, 23.01.2005. Abgerufen am 25.09.2014 von http://www.businessweek.com/stories/2005-01-23/theyre-watching-you
201 http://en.wikipedia.org/wiki/ChoicePoint
202 http://www.lexisnexis.com/risk (Abgerufen am 25.09.2014)
203 http://www.lexisnexis.com/risk/about/data.aspx (Abgerufen am 25.09.2014)
204 http://www.lexisnexis.com/risk/about/default.aspx (Abgerufen am 25.09.2014)

bilien-Eigentümer vor „**Problem-Mietern**“ schützen[205]. Mit dem Identitäts- und Authentifizierungssystem „TrueID®“[206] können Datensätze mit biometrischen Daten von **Fotos** bis zu **Fingerabdrücken** verknüpft werden. Dazu kann die Identität von Personen mit Hilfe einer Datenbank von 34 Milliarden Einträgen aus 10.000 Quellen verifiziert werden und diese Informationen etwa mit **Zahlungs- oder Kundenkarten** verknüpft werden. Darüber hinaus werden sogar biometrische Services zur **Stimmerkennung** angeboten[207]. Der ***Social Media Monitor*** des Produkts „LexisNexis Accurint® for Law Enforcement“ erlaubt die Erkennung von „Risiken und Bedrohungen“ in sozialen Medien und die Identifikation von „Postings und/oder Tweets“[208].

5.3.2. Beispiel: Acxiom

Das US-Unternehmen *Acxiom*[209] verfügt mit bis zu **3.000 einzelnen Eigenschaften** von etwa **700 Millionen Menschen**[210] über einen der größten Bestände an Daten über KonsumentInnen weltweit. Die Firma wurde 1969 unter dem Namen *Demographics Inc* gegründet, um mit den Daten aus öffentlichen Telefonbüchern personalisierte Werbung zu verschicken – unter anderem für Wahlkämpfe der demokratischen Partei. Heute betreut *Acxiom* über 2,5 Milliarden Kundenbeziehungen und betreibt 15.000 Kundendatenbanken von 7.000 Unternehmen aus Bereichen wie **Finanzwirtschaft**, **Versicherung**, **Handel**, **Gesundheit**, **Technologie** oder **Autoindustrie** – unter anderem für 47 der „Fortune 100“ Unternehmen, aber auch für **US-Regierungsbehörden**. Kurz nachdem das FBI die Namen der 19 Attentäter vom 11. September 2001 veröffentlicht hatte, hatte *Acxiom* elf von ihnen in den eigenen Datenbanken identifiziert[211]. *Acxiom* ist seit 2004 auch mit einer **Tochterfirma in Deutschland**[212] aktiv und hat bereits Daten über 44 Mio. Deutsche gesammelt.

Umfangreiche Dossiers

Im „Consumer Data Products Catalog“[213] von *Acxiom* werden hunderte Eigenschaften („Elements“) aufgelistet, die Firmenkunden über Personen oder Haushalte zur Vervollständigung ihrer Kundendatenbanken erwerben können. Neben Basisdaten wie Name, Alter, Geschlecht, Telefonnummern, E-Mail-Adressen stehen umfangreiche Dossiers über **Ausbildung**, **Wohnen**, **Beschäftigung**, **Finanzen**, **Familie**, **Kriminalakten** oder **Wohnungs- und Fahrzeug-Eigentum** zur Verfügung. Allein im Themenbereich „Geographie und Adresse“ werden 25 einzelne Eigenschaften angeboten, im Bereich „ethnische Zugehörigkeit“ zehn Eigenschaften. Darüber hinaus stehen Daten über **Wahlverhalten**, Neigung zum **Glücksspiel** oder „Interessen“ wie **Diät/Gewichtsverlust**, **Casino**, **Lotterie**, **Rauchen/Tabak**, oder **Gewinnspiele** zur Verfügung. Dazu sind Daten über „Bedürfnisse“ im Bereich Gesundheit enthalten – unter anderem in Bezug auf **Allergien**, **Orthopädie**, **Diabetes**, **Cholesterin** oder **Arthritis/Mobilität**.

---

205 Lexis Nexis: Screening Solutions. Abgerufen am 25.09.2014 von https://www.lexisnexis.com/government/solutions/literature/screening.pdf

206 http://www.lexisnexis.com/risk/downloads/literature/trueid.pdf (Abgerufen am 25.09.2014)

207 http://www.lexisnexis.com/risk/products/voice-biometrics.aspx (Abgerufen am 25.09.2014)

208 http://www.lexisnexis.com/risk/newsevents/press-release.aspx?id=1381851197735305 (Abgerufen am 25.09.2014)

209 http://en.wikipedia.org/wiki/Acxiom

210 Acxiom Corp., Annual Report 8. 2013. Abgerufen am 10.07.2014 von http://d3u9yejw7h244g.cloudfront.net/wp-content/uploads/2013/09/2013-Annual-Report.pdf

211 Behar, Richard (2004): Never Heard Of Acxiom? Chances Are It's Heard Of You. Fortune Magazine, 23.02.2004. Abgerufen am 10.07.2014 von http://archive.fortune.com/magazines/fortune/fortune_archive/2004/02/23/362182/index.htm

212 Mclaughlin, Catriona (2013): Acxiom. Die Besserwisser. Die Zeit, 05.07.2013. Abgerufen am 10.07.2014 von http://www.zeit.de/2013/28/acxiom/komplettansicht

213 Acxiom: The Power of Insight: Consumer Data Products Catalog. Abgerufen am 10.07.2014 von https://www.hashdoc.com/documents/8135/data-products-catalog

Sortieren und klassifizieren

Mit dem Analyse- und Segmentierungs-System „Personicx“ werden Haushalte auf Basis von Konsumverhalten und demographischen Informationen zu einer oder mehreren von **1.270 Gruppen** zugeordnet, die deren **Lebensstil** beschreiben. Untermodule wie „Personicx Hispanic“, „Personicx Insurance Groups“ oder „Personicx LifeChanges“ bieten Daten über spezifische Zielgruppen. „Personicx“ wird inzwischen offenbar nicht mehr einzeln angeboten, sondern ist nun Teil des „Acxiom Audience Operation System“[214]. Dieses System ermöglicht laut *Gartner* einen umfassenden Blick auf die „Audience“, über Online- und Offline-Aktivitäten, über Kanäle und Geräte hinweg – auf Basis „nicht duplizierter“ Datensätze, die mit detaillierten demographischen, kontextuellen, sozialen Profilen und Daten über das Verhalten angereichert sind[215].

Verknüpfung von Online und Offline

Acxiom bietet Services, die eine eindeutige **Identifikation von KonsumentInnen** ermöglichen, wenn Kunden an der Kasse nach der Postleitzahl gefragt werden – und ein Name von einer Zahlung mit Scheck oder Kreditkarte zur Verfügung steht[216] (vgl. Singer 2012). Im Rahmen von Partnerschaften mit ***Facebook***[217] und ***Twitter***[218] arbeitet das Unternehmen daran, gezielte Anzeigen in sozialen Netzwerken auf Basis von Einkäufen in Geschäften zu schalten. Außerdem ist *Acxiom* Teil eines Pilotprogramms von ***Google***, bei dem Klicks aus den Werbenetzwerken von *Google* mit dem Ladenverkauf verknüpft werden sollen. 2014 hat Acxiom den Kauf der Firma ***Liveramp*** bekanntgegeben, die auf die Verknüpfung von bestehenden Kundendatenbanken mit Online-Nutzungsvorgängen spezialisiert ist[219] und mit März 2014 laut Eigenangabe **drei Milliarden Kundendatensätze „ins Web gebracht“** hat. Im Firmenblog[220] wird der Prozess wie folgt erklärt: Kunden-Unternehmen senden große Datensätze mit Namen und Schlüsselfeldern wie Postanschriften oder E-Mail-Adressen, *Liveramp* verknüpfe daraufhin diese Daten mit Daten, die „nur“ mit einem Browser oder einem Gerät assoziiert seien.

In der Analyse von *Gartner* (2013) über das „Audience Operating System“ von *Acxiom* wird hervorgehoben, dass damit eine Technologie zur Verfügung stünde, die individuelle Profile aus unterschiedlichen Kanälen und Geräten verknüpfen könne, indem persönliche Daten miteinander in Beziehung gesetzt werden. Die umstrittene Praxis, mit der heute hunderte Unternehmen das Verhalten der NutzerInnen über mehrere Websites hinweg mit Hilfe von auf deren Browsern gespeicherten *Cookies* aufzeichnen würden, wäre mit der Technologie von *Acxiom* hinfällig. Durch Verzicht auf *Cookies* hätte diese Technologie einen gewissen „Privacy Appeal“, allerdings wäre unklar, wie die „Privacy Community“ auf diese Art des Einsatzes persönlicher Daten reagieren werde. Das Risiko wäre hoch, dass Unternehmen oder KonsumentInnen diese Technologie „missbrauchen, misstrauen oder missverstehen“ könnten. Als Fazit wird empfohlen, dass EntrepreneurInnen und InvestorInnen strategische Optionen für ein „wahrscheinlicher werdendes“ Szenario bedenken sollten, in dem „Third Party Cookies“ durch von Unternehmen wie *Acxiom*

214 http://aos.acxiom.com/aos-analytics (Abgerufen am 10.07.2014)

215 Frank, Andrew; Kihn, Martin (2013): Acxiom's Audience Operating System Could Reinvent Data-Driven Marketing. Gartner, 26.09.2013. Abgerufen am 25.09.2014 von https://www.gartner.com/doc/2597521?ref=ddisp

216 Singer, Natasha (2012): You for Sale. Mapping, and Sharing, the Consumer Genome. New York Times, 16.06.2012. Abgerufen am 10.07.2014 von http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html

217 Facebook: New Ways to Reach The Right Audience. 27.02.2013. Abgerufen am 10.07.2014 von https://www.facebook-studio.com/news/item/new-ways-to-reach-the-right-audience

218 Dwoskin, Elizabeth (2014): Data Broker Acxiom Moves to Tie Physical World to Online Data. Wall Street Journal, 14.05.2014. Abgerufen am 10.04.2014 von http://blogs.wsj.com/digits/2014/05/14/data-broker-acxiom-moves-to-tie-physical-world-to-online-data

219 Kaye, Kate (2014): Acxiom Acquires LiveRamp to Boost Offline-to-Online Data Capability. Advertising Age, 14.05.2014. Abgerufen am 10.07.2014 von http://adage.com/article/datadriven-marketing/acxiom-buys-liveramp-offline-online-data-capability/293212/

220 http://blog.liveramp.com/2012/10/03/data-onboarding-system-overview (Abgerufen am 10.07.2014)

oder *Google* betriebene „large data exchanges“ ersetzt werden.

5.4. Online Tracking und Werbenetzwerke: Die unbekannte Macht

Neben traditionellen großen Datensammel-Unternehmen wie *Acxiom*, die oft schon viele Jahrzehnte existieren, gibt es viele neue Player im Bereich Online-Tracking und Werbung, die gewaltige Mengen an persönlichen Informationen sammeln. Viele der beteiligten Firmen sind in der Öffentlichkeit weitgehend unbekannt, zeichnen aber oft **jeden unserer Klicks** und **jede unserer Interaktionen** im Internet und auf mobilen Geräten auf.

Verhalten im Netz und in mobilen Apps

Die meisten dieser Services können mittels kleiner Code-Fragmente einfach in Websites oder *Apps* eingebaut werden und übertragen ab diesem Zeitpunkt Daten über das Verhalten der NutzerInnen an Dritte. Diese Code-Fragmente werden als **Zählpixel**, ***Web Beacons*** oder ***Web Bugs***[221] bezeichnet und können mit Hilfsmitteln wie der Firefox-Erweiterung *Lightbeam*[222] sichtbar gemacht werden. Nach der Installation von *Lightbeam* wird beim Aufruf einer beliebigen Website sichtbar, an welche Drittparteien Daten übertragen wurden. Viele dieser Services speichern ***Cookies***[223] auf den Rechnern der NutzerInnen, um sie später wiederzuerkennen. Diese Cookies können beispielsweise mit der Browser-Erweiterung *Ghostery*[224] sichtbar gemacht werden - dieses Tool kann auch dabei helfen, die permanente Datenübertragung an Dritte zu verhindern. Manche Tracking-Services verzichten aber inzwischen auf Cookies und setzen zur Wiedererkennung der NutzerInnen auf sogenannte **Browser- oder Geräte-Fingerabdrücke**[225].

Übermittlung an bis zu 234 Drittparteien

Das *Wall Street Journal* hat bei einer aufwändigen Untersuchung der 50 populärsten Websites schon 2010 festgestellt, dass bis auf *Wikipedia* alle davon auf derartige Weise die Daten ihrer NutzerInnen an Dritte übertragen (vgl. Wall Street Journal 2010). **37 der 50 populärsten Websites** haben 2010 bei jedem Klick Informationen an **über 30 Drittparteien** übertragen, 22 davon sogar an über 60 Drittparteien. Spitzenreiter ist die Website *dictionary.com*, die 2010 bei jedem Seitenaufruf Daten an 234 externe Services übertragen hat.

Deutsche Nachrichten-Portale

Eine Untersuchung[226] aus dem Jahr 2014 hat festgestellt, dass folgende Auswahl populärer deutscher Nachrichten-Websites bei jedem Klick Nutzungsdaten an **bis zu 59 externe Services** überträgt:

Die Welt	Bild	Spiegel	Heise Online	Süddeutsche	Zeit Online	FAZ	Tagesspiegel	Tagesschau
59	44	33	19	47	37	55	37	4

Tabelle 16: *Anzahl der Dritt-Unternehmen, an die beim Aufruf von deutschen Nachrichten-Websites NutzerInnendaten übertragen werden. Quelle: http://newsreadsus.okfn.de*

Diese Dritt-Unternehmen, an die die Daten der Website-BesucherInnen übertragen werden, sind entweder **Werbenetzwerke** oder **Web-Analyse-Dienste**, aber auch viele andere Services wie

221 http://en.wikipedia.org/wiki/Web_bug
222 https://www.mozilla.org/de/lightbeam/
223 http://de.wikipedia.org/wiki/Cookie
224 Ghostery steht für die Browser Firefox, Chrome, Opera und Safari zur Verfügung: https://www.ghostery.com
225 http://en.wikipedia.org/wiki/Device_fingerprint
226 @stefanwehrmeyer, @annabelchurch, @pudo (2014): We used to read the newspaper, now the news reads us. Abgerufen am 18.09.2014 von http://newsreadsus.okfn.de/

Google, *Facebook* oder *Twitter*. *Google* und deren unzählige Services wie *Google Analytics*[227] oder die Werbenetzwerke *DoubleClick*[228] oder *AdMob*[229] sind beinahe auf jeder Website eingebunden. *Facebook* ist beispielsweise überall dort eingebunden, wo auf einer Website ein *Facebook-Like-Button* sichtbar ist.

Tausende Unternehmen

Darüber hinaus existieren tausende Unternehmen und Services, an die sowohl bei Website-Besuchen als auch bei der Nutzung von *Smartphone-Apps* persönliche Daten übertragen werden. Die Situation ist sehr unübersichtlich und intransparent, über viele dieser Unternehmen ist sehr wenig bekannt und es gibt keine systematische Forschung dazu. Der Anbieter *segment.io*[230] wirbt beispielsweise damit, dass durch den Einbau von deren Service in Websites oder *Apps* die Daten der NutzerInnen unkompliziert und automatisiert gleich an **über 100 andere Dritt-Unternehmen** weitergeleitet werden können – ohne dass dies für NutzerInnen in irgendeiner Weise erkennbar oder nachvollziehbar ist. Da für *segment.io* aber jede Integration mit einem Dritt-Anbieter ein gewisser Aufwand ist, kann die folgende Liste von Services vielleicht zumindest ansatzweise Überblick in diesen Sektor bringen:

Werbung	**Analytics**	**Customer Relationship Management (CRM)**	**User Testing**
AdLearn Open Platform, AdRoll, AdWords, AppNexus, awe.sm, Bing Ads, comScore, Facebook Conversion Tracking, Facebook Custom Audiences, Flurry, Millennial Media, Nanigans, Perfect Audience, Quantcast, Rockerbox, Rocket Fuel, ShareASale, Simpli.fi, Tapstream, TellApart, Twitter Ads, Google Tag Manager, SaaSquatch, Alexa, Convertro, DataXu, Evergage, Hello Bar, Kenshoo, MediaMath	Iron.io, Keen IO, Librato, Lytics, Webhooks, Amplitude, AppsFlyer, Clicky, CommandIQ, Countly, Flurry, FoxMetrics, Frontleaf, Gainsight, Google Analytics, GoSquared, Heap, HubSpot, KISSmetrics, Localytics, Mixpanel, Omniture, Piwik, TestFlight, Totango, trak.io, USERcycle, Woopra, Yandex Metrica, Chartbeat, ChurnBee, Gauges, Improvely	Awesomatic, Get Satisfaction, Help Scout, Intercom, LiveChat, Lucky Orange, Olark, Preact, SnapEngage, UserVoice, Zendesk, LeadLander, Salesforce, StackLead, trak.io **Ecommerce** Bronto, Curebit, FoxMetrics, Google Analytics, GoSquared, Mojn, Monetate	Iterable, Optimizely, Taplytics, Visual Website Optimizer, Crazy Egg, Inspectlet, Lucky Orange, Mouseflow, MouseStats, Navilytics, Get Satisfaction, Mixpanel, Qualaroo, UserVoice, WebEngage **E-Mail-Marketing** Bronto, CommandIQ, Curebit, Customer.io, Drip, Eloqua, Email Aptitude, HubSpot, Intercom, Iterable, Klaviyo, MailChimp, Marketo, Mixpanel, Outbound, Pardot

Tabelle 17: *segment.io überträgt die Klick-Daten von Website-NutzerInnen an bis zu 100 weitere Dritt-Anbieter. Quelle: https://segment.io/integrations*

Auf der Website des Privatsphäre-Dienstleisters *Ghostery* findet sich eine Liste mit fast **2000 Unternehmen**[231], an die regelmäßig Daten von Websites oder Apps übertragen werden. Die Liste enthält Tätigkeitsbereiche und Kurzbeschreibungen der Unternehmen sowie teils Informationen über die Datennutzung, Links zu *Privacy Policies* und Möglichkeiten zum *Opt-Out*.

5.4.1. Beispiel: Flurry

Die „Mobile Analytics" und Werbe-Plattform *Flurry*[232] wurde im Sommer 2014 von *Yahoo* gekauft und betreibt ein System, das umfangreiche Informationen über das Verhalten von *Smartphone*-NutzerInnen sammelt und *App*-Herstellern anbietet, ihre NutzerInnen zu analysieren und mit zielgerichteter Werbung und anderen Methoden Geld zu verdienen. *Flurry* wird laut Eigenanga-

227 http://de.wikipedia.org/wiki/Google_Analytics
228 http://de.wikipedia.org/wiki/DoubleClick
229 http://en.wikipedia.org/wiki/AdMob
230 https://segment.io/integrations (Abgerufen am 18.09.2014)
231 http://www.ghosteryenterprise.com/company-database/ (Abgerufen am 18.09.2014)
232 http://en.wikipedia.org/wiki/Flurry_(company)

be[233] in **540.000 *Apps*** auf *iOS*, *Android* und anderen Plattformen genutzt, ist damit global auf über **1,4 Milliarden *Smartphones* und *Tablets*** installiert und zeichnet monatlich die Daten von 165 Milliarden einzelnen Nutzungs-Sessions auf. Damit besitzt das Unternehmen laut *Forbes*[234] einen „Schatz aus mobilen *App*-NutzerInnen-Daten mit einer höheren Reichweite als Google oder Facebook."

1,4 Milliarden Smartphones und Tablets

Flurry wirbt damit, **ein Drittel aller globalen *App*-Aktivität** zu vermessen und Zugriff auf durchschnittlich 7 *Apps* auf über 90% aller Endgeräte weltweit zu besitzen. Die NutzerInnen werden über *Apps* und Geräte hinweg wiedererkannt. Mit den gesammelten Daten aus den genutzten *Apps* könne ein „reichhaltiges Bild über die Interessen einer Person" gewonnen werden. Die Plattform bietet diverse Segmentierungs-Möglichkeiten und die gezielte Ansprache von NutzerInnen nach Kriterien wie **Interessen**, **Geschlecht**, **Alter**, **Sprache**, **Gerät**, **Betriebssystem** - und nach sogenannten „Personas"[235] wie **Hardcore-Gamer**, **Finanz-Geeks**, **neue Mütter**, **Slots Players** oder **LGBT** (also schwule oder lesbische Personen). Diese „Personas" und andere Daten werden aus dem *App*-Nutzungsverhalten berechnet. Seit Frühjahr 2014[236] arbeitet *Flurry* mit dem Marktforschungs- und Konsumentendaten-Unternehmen ***Research Now***[237] zusammen, das neben Umfragen unter anderem auch ein Hotel- und Flug-Bonusprogramm betreibt. *Flurry* kombiniert deren Daten mit dem eigenen Bestand und bietet seither 350 weitere „Offline-Datenpunkte" und „Profil-Attribute" über **Demographie**, **Interessen** und **Lifestyle** an (z.B. über **Einkommen** oder **Kinder**).

Gezielte Ansprache von NutzerInnen

Viele *App*-EntwicklerInnen setzen anfangs nur die kostenlose Version von *Flurry* ein. Der Einbau ist unkompliziert und ermöglicht die Analyse des *App*-Nutzungsverhaltens. Danach kann die Plattform entweder zur Monetarisierung der eigenen *App* genutzt werden – also als Werbemöglichkeit für andere zur Verfügung gestellt werden. Oder es wird selbst gezielte Werbung für die eigene *App* gebucht – etwa in Form von Werbebannern, Videos oder kurzen Unterbrecher-Spots. Die Preise werden wie bei anderen Online-Werbeplattformen via Echtzeit-Auktion gehandelt. *Flurry* bietet außerdem ***Re-Targeting*** an, also die Wiedererkennung von NutzerInnen, die etwa eine Registrierung oder eine Bestellung in der *App* abgebrochen haben. Diese können in der Folge gezielt angesprochen werden – auch in anderen *Apps* oder mobilen Websites.

---

233 http://www.flurry.com/solutions/advertisers/brands (Abgerufen am 18.09.2014)

234 Olson, Parmy (2013): Meet The Company That Tracks More Phones Than Google Or Facebook. Forbes, 30.10.2013. Abgerufen am 18.09.2014 von http://www.forbes.com/sites/parmyolson/2013/10/30/meet-the-company-that-tracks-more-phones-than-google-or-facebook/

235 http://www.flurry.com/sites/default/files/resources/Personas%20vF.pdf (Abgerufen am 18.09.2014)

236 Bergen, Mark (2014): Flurry Launches Service to Track Mobile App Users, Offline The Analytics Firm Partners With Research Now, As the Race to Target Inside Apps Picks Up. Advertising Age, 24.03.2014. Abgerufen am 18.09.2014 von http://adage.com/article/digital/flurry-research-build-mobile-app-advertising-database/292287/

237 http://en.wikipedia.org/wiki/Research_Now

6 Schlussfolgerungen

„[W]enn wir alle, als Gesellschaft, beschließen, dass wir ein derartiges Verhalten unterlassen sollten, dann würde die Tatsache, dass jeder sofort weiß oder wissen kann, wer sich so verhält, verhindern, dass sich überhaupt jemand so verhält"
Aus dem Roman „The Circle" von Dave Eggers (2014)

„Ihr müsst für eure Privatsphäre kämpfen, oder ihr werdet sie verlieren"[238]
Eric Schmidt, Google, 2013

In den vorangegangenen Kapiteln wurde der Versuch unternommen, anhand von Beispielen und ausgewählten Problemfeldern einen fundierten Überblick über aktuelle Praktiken und internationale Trends im Feld der kommerziellen digitalen Überwachung im Alltag zu gewinnen. Im folgenden Kapitel werden die Situation und deren gesellschaftliche Implikationen zusammengefasst und daraus Handlungsempfehlungen für Politik, Öffentlichkeit, Zivilgesellschaft und BürgerInnen abgeleitet.

6.1. Erfassung, Verknüpfung und Verwertung persönlicher Daten im Zeitalter von Big Data

Facebook hatte im Juni 2014 global 829 Millionen - zumindest einmal täglich aktive - NutzerInnen[239] und wertet in jeder Sekunde Millionen von Einzelinformationen über deren Kontakte, Interessen und Verhalten aus. ***Google*** gibt wenige Zahlen über registrierte NutzerInnen heraus, dürfte aber allein infolge der globalen Dominanz auf dem Suchmaschinen-Markt und einem *Android*-Marktanteil von fast 80% bei einer Milliarde verkaufter *Smartphones* 2013 Zugriff auf ähnliche Mengen täglicher Nutzungsinteraktionen kommen. Die *Smartphone*-Werbeplattform ***Flurry*** zeichnet jede Nutzungsaktivität in 540.000 *Apps* auf 1,4 Milliarden Endgeräten auf. Bei einem hohen Anteil von Websites wird jeder Klick an bis zu 200 Dritt-Unternehmen gleichzeitig übertragen, die meisten populären Websites sind betroffen. NutzerInnen werden über Plattformen, Geräte, *Apps* und Websites hinweg wiedererkannt, insgesamt sammeln global **Tausende von Firmen** Website-Klicks und *App*-Interaktionen der NutzerInnen, der Sektor ist hochgradig intransparent.

Digitale Verhaltensmuster analysieren…

Gleichzeitig lassen sich im Zeitalter von ***Big Data*** mit automatisierten Analyse-Methoden schon aus rudimentären Metadaten über das Online-Verhalten vergleichsweise zuverlässige und umfangreiche Persönlichkeitsprofile erstellen. Dabei wird versucht, mit Technologien des *Data Mining* auf Basis von Statistik und maschinellem Lernen in großen Datenmengen **Muster und Zusammenhänge** zu erkennen – aus Rohdaten wie Einkäufen, Kreditkartenzahlungen, Likes, Kontakten, angehörten Songs, Surf- und Suchverhalten, Standort-Daten, *App*-Nutzungshäufigkeiten, Tastatur-Eingaberhythmus oder der Anzahl, Dauer und Häufigkeit von Anrufen oder SMS. Aus diesen Verhaltensmustern kann – sogar ohne eine Analyse der Kommunikationsinhalte – mit ei-

238 Übersetzung durch den Verfasser, Quelle: Colvile, Rob (2013): Eric Schmidt interview: 'You have to fight for your privacy or you will lose it'. The Telegraph, 25.05.2013. Abgerufen am 10.07.2014 von http://www.telegraph.co.uk/technology/eric-schmidt/10076175/Eric-Schmidt-interview-You-have-to-fight-for-your-privacy-or-you-will-lose-it.html

239 Facebook (2014): Facebook Reports Second Quarter 2014 Results. Abgerufen am 18.09.2014 von http://files.shareholder.com/downloads/AMDA-NJ5DZ/3485478028x0x770575/481ba943-c7b2-4336-9d70-6453934517db/FB_News_2014_7_23_Financial_Releases.pdf

ner gewissen Wahrscheinlichkeit **auf persönliche Eigenschaften geschlossen** werden – etwa auf Geschlecht, Alter, Beruf, Einkommen, ethnische Zugehörigkeit, religiöse und politische Einstellung, sexuelle Orientierung, Schwangerschaft, Lebensstil, Nikotin-, Alkohol- und Drogenkonsum, Schwangerschaft, Lebensstil, Emotionen – und auf Charaktereigenschaften wie Neurotizismus, Extraversion, Offenheit, Gewissenhaftigkeit, soziale Verträglichkeit, kreatives Potenzial, Durchhaltevermögen oder Lernkapazität.

Risiken prognostizieren und Entscheidungen treffen

Mit der Prognose von Charaktereigenschaften aus digitalen Metadaten befassen sich heute nicht nur die Wissenschaft, sondern auch Unternehmen und Geheimdienste. Große **Versicherungen** wie *Aviva* beschäftigen sich mit der Prognose von Risiken für **Krankheiten** wie Diabetes, hohem Blutdruck oder Depression aus Daten über Konsumverhalten, Lebensstil und Einkommen. Unternehmen wie *zest finance*, *Kreditech* oder *Cignifi* prognostizieren Bonität und **Kreditwürdigkeit** aus Standort-Informationen, Telefonie-Verhalten oder Profilen in sozialen Netzwerken. **Werbetreibende** vermessen, segmentieren und klassifizieren ihr Publikum, steigern damit Konversionsraten und Verkäufe - oder sprechen Online-SpielerInnen gezielt in ganz bestimmten emotionalen Momenten zwischen Begeisterung und Frustration an. **Personalabteilungen** bewerten Angestellte und BewerberInnen durch die statistische Analyse umfangreicher Informationen aus Fragebögen, Lebensläufen, Anwesenheits-, Schulungs- und Leistungsdaten. Große **Online-Shops** bieten ihre Produkte zu personalisierten Preisen an oder zeigen unterschiedlich teure Produkte an - abhängig vom Standort der NutzerInnen, von deren Surf-Verhalten oder von anderen individuellen Eigenschaften und Verhaltensweisen. Im Rahmen von ***Business Intelligence*** werden persönliche Daten inzwischen in fast allen Wirtschaftsbereichen zur kundenspezifischen Prognose von Risiken, Ertragschancen oder Loyalität eingesetzt - und daraus Entscheidungen über einzelne Personen abgeleitet.

Der Handel mit persönlichen Daten in den USA

Langjährige internationale Player im Geschäft mit den persönlichen Daten in den USA verfügen über umfangreiche Dossiers über die gesamte Bevölkerung, sammeln laut *Federal Trade Commission* Daten über KonsumentInnen aus umfassenden Online- und Offline-Quellen und speichern diese teils unbefristet - und zwar "größtenteils ohne das Wissen der Konsumenten" (FTC 2014). Die US-Firma ***Acxiom*** speichert etwa bis zu 3.000 einzelnen Eigenschaften von etwa 700 Millionen Menschen, betreibt Kundendatenbanken für Tausende von Unternehmen in den Bereichen Finanzen, Versicherung, Handel, Gesundheit, Technologie oder Autoindustrie, kombiniert diese mit Online-Nutzungsvorgängen und kooperiert mit *Google*, *Facebook* und *Twitter*. Die Risikomanagement-Sparte des Unternehmens ***Lexis Nexis*** verfügt über Daten von 500 Millionen Menschen, arbeiten für Banken, Behörden, Versicherungen, Handel oder den Gesundheitssektor, bietet etwa Informationen über „Problem-Mieter“ oder Hintergrund-Überprüfungen von ArbeitnehmerInnen an und verknüpft biometrische Daten von Fotos bis zu Fingerabdrücken mit Zahlungsdaten und Kundenkarten. Die Firma ***Recorded Future*** erfasst Daten über Personen von fast 600.000 Websites in sieben Sprachen, nutzt diese Informationen, um deren zukünftiges Verhalten vorherzusagen und arbeitet sowohl für Unternehmen als auch für Militär und Geheimdienste - seit 2009 sind unter anderem *Google* und *In-Q-Tel* und damit indirekt der US-Geheimdienst *CIA* an *Recorded Future* beteiligt.

permanente Datenflüsse durch vernetzte Sensoren

Immer mehr **Geräte mit einer Vielzahl an Sensoren** liefern die Basis für diese permanenten Datenflüsse. Neben den in *Smartphones* schon üblichen Sensoren wie Mikrofon, Kamera, *GPS*-Empfänger, Bewegungs-, Lage-, Licht-, Näherungs-, Magnetfeld- oder Fingerabdrucksensoren vermessen Fitness-Tracker, Smartwatches und andere Wearables nicht mehr nur Schritte, Puls oder Schlaf, sondern auch Atmung, Hautwiderstand, Blutdruck oder Blutzucker - und verfügen über Barometer, Temperatur- oder Luftfeuchtigkeitssensoren. Im **Internet der Dinge** werden vernetzte Sensoren allgegenwärtig: *E-Book-Reader* übertragen detaillierte Informationen zum Leseverhalten an Unternehmen, vernetzte TV-Geräte Daten zum Fernsehverhalten. Vernetzte Autos, Stromzähler, Thermostaten, Brandmelder, Kühlschränke oder Badewannen liefern umfassende Daten über unser Alltagsverhalten. Die NutzerInnen überwachen nicht nur sich selbst, sondern auch andere - etwa ihre Kinder oder ihre Angestellten, die entweder Geräte mit Sensoren mit sich tragen oder sich an Orten bewegen, die mit Sensoren ausgestattet sind. Datenbrillen und Wearables zur digitalen Vermessung von Körper, Gesundheit, Verhalten und Umgebung werden unauffälliger - etwa in Form von Pulssensoren in biometrischen Kopfhörern, Temperatur- und Feuchtigkeitssensoren in elektronischen Tattoos oder durch mit Sensoren ausgestattete Ringe, Socken, T-Shirts, Büstenhalter, Zahnbürsten oder Gabeln.

6.2. Gesellschaftliche Implikationen von kommerzieller digitaler Überwachung

Durch aktuelle Informationstechnologie und deren Einsatz wird Überwachung zum beiläufigen Nebenprodukt alltäglicher Transaktionen und Handlungen (vgl. De Zwart 2014). Bei der Betrachtung der im vorigen Kapitel zusammengefassten Entwicklungen wird klar, dass die von David Lyon (1994) beschriebene „Überwachungsgesellschaft" schon längst Realität geworden ist. Das von ihm beschriebene „Social Sorting" in Form einer **ständigen Klassifikation und Sortierung der Bevölkerung** durch Informationstechnologie und Software-Algorithmen auf Basis persönlicher Daten ist heute an der Tagesordnung.

Gesellschaftliche Problematiken und Risiken

Viele dieser Technologien bieten gleichzeitig große Chancen und Möglichkeiten – soziale Netzwerke, Personalisierung oder Empfehlungssysteme haben etwa unseren Alltag auch sehr positiv geprägt. Trotzdem ergeben sich aus den dargestellten Entwicklungen auf mehreren Ebenen massive gesellschaftliche und individuelle Problematiken und Risiken:

- **Kontrollverlust:** Wenn persönliche Daten einmal digital erfasst und gespeichert sind, können sie nur schwer wieder gelöscht oder geändert werden. Viele internationale Datenhandels-Unternehmen speichern persönliche Daten oder daraus abgeleitete persönliche Daten auf unbeschränkte Zeit (vgl. FTC 2014). Außerdem sind durch zeitgenössische Analyse-Technologien scheinbar anonymisierte Daten heute zunehmend de-anonymisierbar. Je mehr einzelne Datenpunkte über eine Person oder deren Verhalten vorliegen, desto eindeutiger lässt sich daraus eine Art „digitaler Fingerabdruck" erzeugen, der zur Identifikation und Wiedererkennung benutzt werden kann.

Intransparente Unternehmen

- **Mangel an Transparenz:** KonsumentInnen können oft nicht nachvollziehen, welche persönlichen Daten über sie und ihr Verhalten von Unternehmen digital erfasst und gespeichert werden, wie diese Daten verarbeitet werden, an wen sie weitergegeben oder verkauft werden, welche Schlüsse daraus gezogen werden und welche Entscheidungen auf Basis dieser Schlüsse über sie gefällt werden. Sowohl die international dominanten Plattformen wie auch kleinere Anbieter von Websites, Services, *Apps* und Plattformen agieren intransparent und informieren die NutzerInnen oft unvollständig, unzugänglich, fehlerhaft oder gar nicht über die Speicherung, Verarbeitung und Verwertung ihrer Daten. Viele Unternehmen ermöglichen den NutzerInnen nicht einmal den vollständigen Zugriff auf ihre eigenen Daten und betrachten ihre Algorithmen als Betriebs- und Geschäftsgeheimnisse (vgl. Weichert

2013).

...eine Frage der Macht

- **Machtungleichgewicht zwischen Unternehmen und NutzerInnen:** Während die NutzerInnen immer transparenter werden, werden die Unternehmen immer intransparenter. Durch die mangelnde Transparenz der von Unternehmen genutzten Daten und Algorithmen sowie durch die nicht vorhandenen Mitbestimmungsmöglichkeiten entsteht eine große Asymmetrie zwischen den NutzerInnen und den Unternehmen, die deren persönlichen Daten verarbeiten, verwerten und damit Profit machen. Darüber hinaus haben nur die Unternehmen selbst Zugriff auf wirklich große Mengen von „sozialen Daten", insbesondere auf die Transaktionsdaten (vgl. Manovich 2011). Dies führt nach Dana Boyd zu einer neuen „digitalen Spaltung" in Bezug auf Fragen wie: „Wer bekommt Zugang? Für welchen Zweck? In welchem Kontext? Und mit welchen Einschränkungen?" (vgl. Boyd et al 2012)

Daten werden in anderen Kontexten eingesetzt

- **Dekontextualisierung:** Persönliche Daten werden zunehmend in völlig anderen Kontexten eingesetzt als die ursprünglichen Verwendungszwecke bei deren Erfassung. Wie Franck Dumortier (2009) argumentiert, motiviert etwa *Facebook* die NutzerInnen dazu, möglichst korrekte, aktuelle und vollständige Informationen anzugeben. Gleichzeitig werden diese Informationen aber für eine große Gruppe von Marketingfirmen und EntwicklerInnen von Dritt-Anwendungen geöffnet. Dadurch können die Daten schlussendlich in ganz anderen Kontexten auftauchen oder genutzt werden als ursprünglich gedacht. Dumortier diagnostiziert bei den NutzerInnen eine Diskrepanz zwischen dem „imaginierten" und dem „wirklichen" Publikum. Dazu muss noch nicht einmal die intuitiv überhaupt nicht mehr nachvollziehbare Situation eintreten, in der Daten aus sozialen Netzwerken etwa gar zur Prognose der Kreditwürdigkeit eingesetzt werden.

Wer sich falsch verhält...

- **Fehlerhafte Daten und falsche Prognosen:** Abgesehen von Fehlern in den Rohdaten oder deren Aufzeichnung können Fehler in den Prognosemodellen oder falsche Klassifikationen massive negative Auswirkungen auf Einzelne haben. *Big Data* ist weit von wirklicher Objektivität oder Zuverlässigkeit entfernt (vgl. Boyd et al 2012). Die Prognosen sind prinzipiell unscharf, da sie auf Korrelationen und Wahrscheinlichkeiten beruhen. Wer beispielsweise die falschen Personen kennt, im falschen Bezirk wohnt oder sich in der *Smartphone-App* „falsch" verhält, wird in einer bestimmten Art und Weise klassifiziert und muss die Konsequenzen tragen, ohne Einfluss darauf zu haben. Individuelle Handlungen können so dekontextualisiert oder missinterpretiert werden, die dahinter stehenden Motivationen können nicht erfasst werden (vgl. De Zwart 2014). Ein Prognosemodell könnte etwa nahe legen, dass durch den Kauf eines bestimmten Produkts die Wahrscheinlichkeit höher ist, dass eine Person eine bestimmte Partei wählt, kann aber niemals eine Erklärung dafür bieten. Wenn durch derartige Modelle auf Basis digitaler Daten über das Verhalten etwa Prognosen über Risiken für Unzuverlässigkeit, Zahlungsunfähigkeit, Krankheit oder Kriminalität erstellt werden, können die Auswirkungen auf Einzelne gewaltig sein.
- **Diskriminierung, Ausschluss und Individualisierung von Risiko:** Wenn Unternehmen Kriterien wie Geschlecht, Alter, ethnische oder religiöse Zugehörigkeit, Armut oder den Gesundheitszustand in ihre Entscheidungen mit einbeziehen, besteht die Gefahr von Diskriminierung oder Ausschluss ganzer Bevölkerungsgruppen oder -segmente. Diese Gefahr verschärft sich, wenn diese Klassifikationskriterien nicht direkt gewonnen, sondern durch statistische Analysemethoden aus persönlichen Daten berechnet werden – und Unternehmen derartige Prognosen dazu nutzen, um Menschen unterschiedlich zu adressieren, zu behandeln oder auszuschließen (vgl. Lyon 2003). Die Chancen, Optionen und Wahlmöglichkeiten von Einzelnen können dadurch eingeschränkt werden - von der Frage, welche Werbung und welche Angebote jemand bekommt, über Preisdiskriminierung bis zu lebensentscheidenden Fragen in den Bereichen Finanzen, Gesundheit, Versicherung oder Arbeit. Michael Fertik diagnostiziert im *Scientific American*, dass durch individuelle Preise und personali-

sierte Angebote die „Reichen“ ein „anderes Internet als die Armen“ sehen würden. (vgl. Fertik 2013). Mit Technologien des *Data Mining* sind Unternehmen in der Lage, profitable KundInnen statistisch zu identifizieren und das exakte Minimum an notwendiger Handlung zu berechnen, mit dem diese KundInnen loyal gehalten werden können (vgl. Palmås 2011). Sogar die US-amerikanische *Federal Trade Commission* befürchtet, dass KonsumentInnen mit bestimmten Verhaltensweisen in Zukunft als „riskanter“ eingeschätzt werden und dadurch höhere Versicherungsprämien anfallen könnten (vgl. FTC 2014). Darüber hinaus könnten „mögliche Diskriminierungseffekte“ nicht einmal mehr nachzuvollziehen sein, wenn wir „keine Entscheidungsmacht“ mehr über die „Wege unserer eigenen Daten“ haben (vgl. Albrecht 2014). Auch Verweigerung der Teilnahme kann Konsequenzen haben: Wenn keine oder zu wenige Daten über eine Person vorhanden sind, schätzt ein Unternehmen das Risiko für eine Kundenbeziehung unter Umständen prinzipiell als zu hoch ein. Wenn Versicherungsunternehmen die Risikoabschätzung von Lebensgewohnheiten und Verhaltensweisen abhängig machen, wird außerdem Risiko individualisiert (vgl. Lyon 2003).

Mit vorauseilendem Gehorsam in die „Datenkatastrophe“?

- **Bedrohung von Freiheit, Demokratie und der Autonomie des Einzelnen:** Wenn Kommunikation und Verhalten permanent digital erfasst und ausgewertet werden, hat dies einen Einfluss darauf, wie sich Einzelne verhalten und wie sie miteinander kommunizieren – nicht nur in Bezug auf soziale oder politische Themen. Dadurch sind die Ausübung demokratischer Rechte und die intellektuelle Freiheit bedroht – und es entsteht die Gefahr, dass Menschen nicht mehr mit „neuen, kontroversen oder devianten Ideen“ experimentieren (vgl. Richards 2013). Viele der 1.606 in der Studie des *Pew Research Center* (2014) befragten globalen ExpertInnen erwarten, dass Anreize zur Verhaltensänderung zum zentralen Treiber für das Internet der Dinge werden - beispielsweise zum Kauf eines Produkts oder zur Anregung von gesünderen oder sichereren Lebensweisen, bestimmten Arbeitsweisen oder der effizienteren Nutzung öffentlicher Güter. Dies könnte substanzielle Auswirkungen auf die Möglichkeit der Menschen, ihr „eigenes Leben zu kontrollieren“, haben. Der prominente Netztheoretiker Evgeny Morozov identifiziert eine „Ideologie des Datenkonsums“, die darauf basiert, dass NutzerInnen ihre persönlichen Daten gegen die scheinbar kostenlose Nutzung von Services oder Geräten tauschen – und die „enorme politische und moralische Konsequenzen“ hätte. Er warnt vor einer mit der „Umweltkatastrophe“ vergleichbaren „Datenkatastrophe“, die uns in einer Welt erwartet, in der persönliche Daten wie Kaffee oder jede andere Ware gehandelt werden“. Wenn sich erst einmal die Hälfte der Bevölkerung freiwillig dafür entschieden hätte, ihr Verhalten permanent digital überwachen zu lassen und im Gegenzug etwa von niedrigeren Versicherungsprämien zu profitieren, würden diejenigen, die nicht damit einverstanden sind, automatisch verdächtig und damit in ihren Möglichkeiten eingeschränkt (vgl. Morozov 2013).

Konkretes Problem

- **Welche Daten sind öffentlich?** Viele Informationen in sozialen Netzwerken sind in der Standardeinstellung öffentlich für alle im Netz zugänglich – in manchen Fällen sogar zwingend (z.B. *Tweets*, *Likes* auf Facebook). Angesichts der weitreichenden Identifikations- und Analysemöglichkeiten stellt sich hier die Frage: Sollen diese „öffentliche" Informationen wirklich uneingeschränkt und ohne Einwilligung von Unternehmen oder für die Forschung verwendet werden dürfen? (vgl. Boyd et al 2012)

Gesellschaftliche Regeln

- **Weitgehende Missachtung von Datenschutzgesetzen durch Unternehmen:** Viele Praktiken von dominanten internationalen Unternehmen in Netz und Mobiltechnologie sind nach den geltenden Gesetzen in Österreich, Deutschland bzw. generell in Europa illegal, die Gesetze werden aber nicht entsprechend durchgesetzt und sanktioniert (vgl. Schrems 2014).
- **Datenmissbrauch und Identitätsdiebstahl:** Überall, wo große Datenmengen gespeichert werden, besteht das Risiko von Datenmissbrauch und -verlust. Beinahe tägliche Medienberichterstattung über Sicherheitslücken und den Verlust von Millionen von NutzerInnen-Datensätzen ist inzwischen Normalität - sogar die größten Unternehmen sind betroffen[240]. Daraus entstehen massive Risiken für Einzelne – von Belästigung und Stalking bis Identitätsdiebstahl und Cyber-Kriminalität.
- **Staatlicher Zugriff auf die von Unternehmen gesammelten Daten:** Im digitalen Zeitalter ist die Privatsphäre gleichermaßen durch private Unternehmen wie auch durch staatliche Behörden bedroht (vgl. De Zwart 2014). Nicht nur die Enthüllungen von Edward Snowden haben gezeigt, dass auch staatliche Behörden und Geheimdienste gern auf die von Unternehmen über BürgerInnen gesammelten persönlichen Daten zugreifen.

Wirtschaftliche Folgen?

- **Verlust des Vertrauens in Kommunikationstechnologie:** Durch die gegenwärtigen Praktiken der allgegenwärtigen Überwachung besteht nicht zuletzt die Gefahr, dass Menschen Informations- und Kommunikationstechnologien zunehmend negativ erleben, das Vertrauen in sie verlieren oder sich gar ganz von ihr abwenden (vgl. WEF 2012).

6.3. Handlungsempfehlungen für Politik, Öffentlichkeit, Unternehmen und BürgerInnen

Der digitale Wandel und dessen nachhaltige Auswirkungen auf allen gesellschaftlichen Ebenen schreiten mit einer Geschwindigkeit voran, der viele EntscheidungsträgerInnen mit einer gewissen Ohnmacht und Ratlosigkeit gegenüberstehen. Unternehmen aus dem Silicon Valley und anderen Regionen der Welt sind **mit hohen Kapitalsummen** ausgestattet, treiben die Entwicklung mit permanenten Innovationen voran und **setzen zunehmend die Regeln** – während Politik, Öffentlichkeit, Zivilgesellschaft und BürgerInnen einfach nur zusehen.

Was tun?

Allgegenwärtige digitale Überwachung könnte künftig **drastische Auswirkungen auf Gesellschaft, Demokratie und die Autonomie des Einzelnen** haben. Die NutzerInnen selbst können sich nur teilweise eigenständig vor dieser Art der kommerziellen Überwachung schützen - denn sogar über Menschen, die nicht teilnehmen, werden digitale Profile angelegt. Abgesehen davon besteht ein großer Konsens darüber, dass eine Nicht-Teilnahme an der Informationsgesellschaft keinesfalls das Ziel sein kann. Digitale Kommunikationstechnologien bieten große Chancen und Möglichkeiten in vielen gesellschaftlichen Bereichen. Um die möglichen negativen Implikationen und die damit einhergehenden gesellschaftlichen Risiken zu minimieren, wird - unterteilt in die Bereiche Politik, Datenschutz, Unternehmen und Wirtschaft, NutzerInnen - folgendes empfohlen:

240 Siehe z.B. das Projekt „DataLossDB", das von Jan. bis Aug. 2014 über 1.000 Vorfälle von Datenverlust mit 502 Millionen involvierten persönlichen Datensätzen verzeichnet: http://datalossdb.org (Abgerufen am 29.09.2014)

Politik und Öffentlichkeit:

Was kann die Politik tun?

- **Transparenz schaffen:** Tausende Unternehmen sammeln heute sehr weitgehende persönliche Daten über Einzelne. Gleichzeitig ist über weite Strecken völlig intransparent, wie diese Informationen gesammelt, analysiert, verknüpft und verwertet werden. Die Behebung dieses Transparenzdefizits muss hohe Priorität haben – durch Forschung, Öffentlichkeit und Regulierung.
- **Dezentrale Technologien fördern und Anreize setzen:** Unternehmen wie *Google* oder *Facebook* und viele andere dominante Plattformen agieren zentralisiert und intransparent. Die Erforschung und Entwicklung von dezentralen Alternativen, die den NutzerInnen mehr Kontrolle über ihre persönlichen Daten einräumen, sollte massiv unterstützt werden. Dabei ist nicht etwa ein „europäisches Google" gemeint, sondern die Entwicklung dezentraler Infrastruktur in Form von offenen und transparenten Services, Protokollen und Algorithmen (vgl. z.B. den Ansatz in Kapitel 4.4.). Die Entwicklung von Datenschutz-affinen Technologien, Services und Geschäftsmodellen im Sinne von „Privacy by Design" sollte auf allen Ebenen der Forschungs-, Förderungs- und Vergabepraxis unterstützt oder sogar zum zwingenden Kriterium gemacht werden. Bei der Entwicklung dezentraler Infrastruktur in Form von offenen und transparenten Services, Protokollen und Algorithmen sollte nicht nur auf Unternehmen oder die etablierte Wissenschaft gesetzt werden, sondern auch das Potenzial der unabhängigen Netz-Community genutzt werden.
- **Kritischen Diskurs und digitale Zivilgesellschaft stärken:** Unternehmen, Technologie und Realität sind der öffentliche Debatte weit voraus. Es braucht einen intensiveren öffentlichen Diskurs über die Chancen, Risiken und Machtungleichgewichte im Zeitalter von *Big Data* sowie über die künftigen gesellschaftlichen Rahmenbedingungen – nicht nur im Bereich der Analyse und Verwertung persönlicher Daten. Die Umweltschutzbewegung gilt oft als Vorbild für eine digitale Zivilgesellschaft. Der Organisations- und Professionalisierungsgrad von zivilgesellschaftlichen Organisationen mit Fokus auf digitale Technologien und deren gesellschaftliche Implikationen in Deutschland ist mangelhaft - die Finanzkraft ist etwa im Vergleich zur Umweltschutzbewegung vernachlässigbar (vgl. Dobusch 2014). In Österreich sieht es nicht viel besser aus.
- **Digitale Kompetenzen stärken:** Das Wissen über mögliche langfristige Auswirkungen unseres heutigen Umgangs mit den eigenen persönlichen Daten ist mangelhaft. Sowohl der bewusstere Umgang mit den eigenen Daten, das Verständnis über Chancen und Risiken digitaler Kommunikationstechnologien als auch die Fähigkeit zur Reflexion des eigenen Mediennutzungs- und Konsumverhaltens müssen gefördert werden. Die Vermittlung digitaler Kompetenz darf sich nicht nur auf eine praktische Ebene beschränken (z.B. „Wie bediene ich ein Textverarbeitungs-Programm").
- **Staat mit Vorbildwirkung:** Politik und staatliche Behörden sollten bei allen Fragen, die die digitale Verarbeitung von persönlichen Daten betreffen, eine Vorreiterrolle einnehmen. Die Vorratsdatenspeicherung war ein unnötiger Eingriff in die Grund- und Bürgerrechte, eine etwaige Wiedereinführung ist strikt abzulehnen. Projekte wie die elektronische Gesundheitsakte ELGA, das Auto-Notrufsystem *eCall* oder der intelligenter Stromzähler („Smart Meter") sollten unter Einbindung von KritikerInnen umfangreich auf mögliche negative Implikationen untersucht werden.

Datenschutz und europäische Datenschutz-Grundverordnung:

Gesetzliche Rahmenbedingungen

- **Ausgangsbasis:** Eine umfassende Behandlung von datenschutzrechtlichen Fragen würde den Rahmen dieser Studie sprengen. Die Entwicklung geeigneter gesetzlicher Rahmenbedingungen ist angesichts der beschriebenen Realitäten und Praktiken keine leichte Aufgabe. Drei Dinge sind weitgehend Konsens: 1) Aktuell klafft eine große Lücke zwischen geltenden Datenschutzgesetzen und der Praxis, in der nicht nur internationale Unternehmen sehr weitgehend gegen geltende Gesetze verstoßen. 2) Aktuelles Recht wird oft nicht durchgesetzt, die Kontrollbehörden haben nicht ansatzweise genügend Ressourcen, 3) Die geltende Datenschutzgesetzgebung ist veraltet und nicht ausreichend an das digitale Zeitalter angepasst.
- **Maximale Aufmerksamkeit und große gesellschaftliche politische Anstrengung:** Die schon seit Jahren diskutierte europäische Datenschutz-Grundverordnung wird sehr weitreichend darüber entscheiden, in welcher Art von Informationsgesellschaft wir in Zukunft leben werden. Dieser Grundsatzentscheidung muss maximale Aufmerksamkeit gewidmet werden. Hier bedarf es einer großen gesellschaftlichen und politischen Anstrengung - und die Verordnung sollte trotzdem möglichst zügig in Kraft treten. Das EU-Parlament hat bereits seinen Beitrag geleistet, nun ist der europäische Rat in Form der VertreterInnen der Mitgliedsstaaten am Zug.
- **Ausgestaltung der europäischen Datenschutz-Verordnung:** Zentrales Augenmerk sollte auf eine gute Ausgestaltung der „informierten Zustimmung" der Betroffenen zur Verarbeitung ihrer persönlichen Daten sowie auf deren Rechte auf Auskunft, Richtigstellung und Löschung gelegt werden. Ebenso wichtig sind die (internationale) Durchsetzbarkeit[241], die Sanktionierung und die Ausstattung der Kontrollbehörden mit angemessenen Ressourcen. Einer der entscheidenden Punkte ist die Abgrenzung von „identifizierbaren" persönlichen Daten von „anonymen" Daten. Viele scheinbar anonymisierte Daten können heute technisch wieder de-anonymisiert werden.
- **Kleine Lücken mit großen Auswirkungen:** Im Zuge der Debatte um die europäische Datenschutz-Grundverordnung wurden von EU-ParlamentarierInnen 3.132 Änderungsanträge zum Gesetzestext eingebracht. Die Plattform *LobbyPlag*[242] stellt alle Änderungsanträge, Quellen und sogar Einschätzung jedes einzelnen Änderungsvorschlags im Hinblick auf eine Stärkung oder Schwächung der Privatsphäre online zur Verfügung und hat 2013 aufgedeckt, dass mehrere Textvorschläge im Wortlaut von IT-Lobby-Organisationen übernommen wurden. Hier besteht die Gefahr, dass bei der Behandlung durch den EU-Ministerrat kleine Gesetzeslücken mit großen Auswirkungen eingebracht werden, die das Potenzial haben, die gesamte Verordnung zahnlos und damit unwirksam zu machen – etwa durch bestimmte Definitionen oder Formulierungen.
- **Transparenz der Algorithmen.** Darüber hinaus wäre darüber nachzudenken, Transparenz rechtlich nicht nur in Bezug auf die gesammelten Daten einfordern, sondern auch bezüglich der eingesetzten statistischen Verarbeitungsalgorithmen. Das betrifft nicht nur die Verarbeitung persönlicher Daten, sondern könnte sich auch auf Algorithmen wie die *Google*-Suche

241 Manche KritikerInnen bezweifeln generell eine internationale Durchsetzbarkeit von Datenschutz-Regulierungen: Einerseits könnten diese Datenflüsse grundsätzlich technisch nicht kontrolliert werden, andererseits könne die Datenverarbeitung jederzeit in Staaten ausgelagert werden, die eine Sanktionierung nicht unterstützen. Hier kann nur entgegengehalten werden, dass mit den gleichen Argumenten die Möglichkeit jeglicher Steuergesetzgebung in Abrede gestellt werden könnte.

242 http://de.lobbyplag.eu/map (Abgerufen am 19.09.2014)

oder den *Facebook*-Newsfeed beziehen.

Unternehmen und Wirtschaft:

Was können Unternehmen tun?

- **„Privacy by Design" und Verschlüsselung:** Die gängige Praxis scheint es oft zu sein, dass auf Verdacht hin möglichst umfassende persönliche Daten erfasst und gespeichert werden. Im Gegensatz dazu sollten Produkte von Beginn an so konzipiert werden, dass dabei nur diejenigen persönlichen Daten verarbeitet werden, die wirklich notwendig sind, dass diese Daten nur dort gespeichert werden, wo es notwendig ist, und dass zuverlässige Anonymisierung einsetzt wird, wo es möglich ist. Auch im Feld *Data Mining* gibt es Ansätze, die auf die Privatsphäre der NutzerInnen Rücksicht nehmen (vgl. z.B. Rakesh 2000). Dort, wo Verschlüsselung auf EndnutzerInnen-Seite möglich und sinnvoll ist, sollte diese durchgehend implementiert werden.
- **„Do Not Track" respektieren:** Das Konzept von *Do Not Track*[243] (DNT) ist inzwischen in den meisten Web-Browsern implementiert und kann einer Website signalisieren, dass die NutzerInnen nicht wünschen, dass über ihre Aktivitäten Profile angelegt werden. Dieser Wunsch ist zu respektieren, derartige Konzepte sollten weiterentwickelt werden.
- **Geschäftsmodelle überdenken:** Das Vertrauen vieler NutzerInnen in digitale Kommunikationstechnologien ist bereits angekratzt. Wie das *World Economic Forum* bereits 2012 festgehalten hat, ist dieser Mangel an Vertrauen in Bezug auf persönliche Daten eine Bedrohung für die digitale Wirtschaft (vgl. WEF 2012). Dem kann von Seite der Unternehmen nur auf eine Weise entgegengetreten werden: Sie müssen Anwendungen und Geschäftsmodelle entwickeln, die verantwortungsbewusst mit den Daten von NutzerInnen umgehen.
- **Wettbewerbsvorteile nutzen:** Durch einen vertrauenswürdigen Umgang mit persönlichen Daten können sich Unternehmen mit ihren Produkten von anderen Unternehmen abgrenzen und sich damit als Alternative positionieren. Vor allem Unternehmen aus Österreich, Deutschland bzw. generell aus Europa arbeiten schon länger unter strengerer Regulierung und sollten diese Erfahrungen nicht nur als Hemmnis, sondern auch als Chance begreifen. Mit Umsetzung der europäischen Datenschutz-Verordnung können sich europäische Unternehmen auch international als vertrauenswürdige und sichere Alternative positionieren.
- **Datenschutz-Gütesiegel und Zertifizierungen:** Durch eine freiwillige Zertifizierung ihrer Produkte als besonders vertrauenswürdig, datensparsam und technisch sicher können Unternehmen einen Wettbewerbsvorteil vor der ungeprüften Konkurrenz erlangen – beispielsweise mit dem europäischen Datenschutz-Gütesiegel EuroPriSe[244].
- **Kommunikation und Aufklärung:** Unternehmen sollten besser über Zweck, Dauer, Umfang und Typen der verarbeiteten persönlichen Daten informieren und die Betroffenen darüber aufklären, wie sie ihre Rechte auf Auskunft, Richtigstellung und Löschung geltend machen können.
- **Unternehmerische und gesellschaftliche Verantwortung übernehmen:** Datenschutzfragen sollten in Zukunft den gleichen Stellenwert erlangen wie Compliance-Themen wie Wettbewerbsrecht oder Korruptionsbekämpfung. Der ethische Umgang mit persönlichen Daten sollte mittelfristig den gleichen Stellenwert erlangen wie Umweltschutz, Diversität oder soziale Verantwortung. Auch die Frage der Überwachung von Angestellten im Unternehmen selbst sollte hier einbezogen werden.

---

243 http://de.wikipedia.org/wiki/Do_Not_Track

244 ITA: Europäisches Datenschutz-Gütesiegel EuroPriSe. Online: http://www.oeaw.ac.at/ita/projekte/europrise/

NutzerInnen:

Was können die NutzerInnen tun?

- **Hilfsmittel einsetzen:** Browser-Erweiterungen wie *Ghostery, Better Privacy, Adblock Plus* oder *Beef Taco* schützen vor Browser-basiertem Online-Tracking und minimieren gleichzeitig störende Online-Werbung. Verschlüsselung ist nicht immer die Lösung, sollte aber überall dort genutzt werden, wo sinnvoll.
- **Datenschutzeinstellungen und Berechtigungssysteme verstehen:** In sozialen Netzwerken und bei anderen Services vorhandene Datenschutzeinstellungen sollten verstanden und genutzt werden, ebenso die Berechtigungssysteme von *Smartphones*, mit denen der Zugriff von *Apps* auf Standort-Daten oder Kontakte geregelt wird.
- **„Unfreundliche" Services, *Apps* und Plattformen meiden:** Nicht jede *App* muss unbedingt genutzt werden, nicht auf jeder Plattform unbedingt teilgenommen werden. Falls doch, sollte vorher zumindest vorher versucht werden, deren Umgang mit persönlichen Daten zu klären. Voraussetzung dafür ist natürlich, dass diese Informationen auch zur Verfügung stehen.
- **„Freundliche" Services, *Apps* und Plattformen nutzen:** Die BetreiberInnen haben nur so lange Macht über deren Services, solange diese auch genutzt werden. Umgekehrt formuliert: Die NutzerInnen haben die Macht. Es gibt beispielsweise Suchmaschinen wie *DuckDuckGo*[245] oder *Ixquick*[246], die auf das Ausspionieren ihrer NutzerInnen verzichten. Wären vor einigen Jahren viele Menschen auf das dezentrale soziale Netzwerk *Diaspora*[247] umgestiegen, könnte das „Problem" *Facebook* und dessen Dominanz heute gar nicht existieren.
- **Datensparsamkeit:** Der umsichtige Umgang mit den eigenen persönlichen Daten sollte obligatorisch sein, aber *Datensparsamkeit* und *Datenvermeidung*[248] sind zweischneidige Schwerter. Viele nützliche und sinnvolle Services sind darauf angewiesen, dass dabei bestimmte persönliche Daten zur Verfügung gestellt werden. Wenn diese Daten oft missbraucht werden, liegt das in der Verantwortung der Unternehmen, die diese Services betreiben.

245 http://de.wikipedia.org/wiki/DuckDuckGo
246 http://de.wikipedia.org/wiki/Ixquick
247 http://de.wikipedia.org/wiki/Diaspora_(Software)
248 http://de.wikipedia.org/wiki/Datensparsamkeit_und_Datenvermeidung

Kurzfassung

Transparente NutzerInnen…

Durch die rasante Weiterentwicklung der Informations- und Kommunikationstechnologien dringt die Erfassung persönlicher Daten und immer mehr in den Alltag ein. Unsere **Vorlieben und Abneigungen** werden heute in einem Ausmaß digital gespeichert, verarbeitet und verwertet, das bis vor wenigen Jahren undenkbar war. Einzelne Personen werden über Geräte und Plattformen hinweg wiedererkannt, deren **Verhalten und Bewegungen** detailliert ausgewertet, **Persönlichkeit und Interessen** akribisch analysiert. Immer mehr Geräte sind heute mit **Sensoren** ausgestattet, mit dem Internet verbunden und ermöglichen so umfassende Einblicke in unser Leben. Gleichzeitig lassen sich im Zeitalter von ***Big Data*** mit automatisierten Methoden schon aus rudimentären Metadaten über Kommunikations- und Online-Verhalten umfangreiche **Persönlichkeitsprofile** erstellen. Aufstrebende Firmen in den Feldern soziale Netzwerke, Online-Werbung, mobile *Apps* oder Fitness arbeiten mit Hochdruck an Geschäftsmodellen, die auf der **kommerziellen Verwertung** der gesammelten Profile beruhen. Internationale Unternehmen agieren dabei teils unter Missachtung regionaler Datenschutzgesetze, oft gilt die Devise: Gemacht wird, was technisch möglich ist - und angenommen wird. In vielen Wirtschaftssektoren von **Marketing und Handel bis Versicherungs-, Finanz- und Personalwirtschaft** herrscht Goldgräberstimmung – und gleichzeitig die Angst, den Anschluss zu verlieren. Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent – deren Services, *Apps*, Plattformen und Algorithmen sind zentralisiert und kaum durchschaubar. Darüber hinaus haben nicht nur die Enthüllungen von Edward Snowden gezeigt, dass auch **staatliche Behörden und Geheimdienste** gern auf die gesammelten Daten zugreifen. Die Privatsphäre ist heute gleichermaßen durch Unternehmen wie auch durch staatliche Behörden bedroht.

...intransparente Unternehmen

Kommerzielle Überwachung?

Die Studie zielte darauf ab, anhand von ausgewählten Problemfeldern und Beispielen einen Überblick über internationale Trends in der zunehmenden Erfassung und Verwertung persönlicher Daten durch Unternehmen zu geben - und **mögliche Auswirkungen auf unser Leben** zu beschreiben. In welcher Form könnte kommerzielle digitale Überwachung zukünftig den Alltag prägen? Was sind die Risiken? Und welche Handlungsoptionen ergeben sich daraus für Politik, Öffentlichkeit, Unternehmen und BürgerInnen? Auf Basis der Forschungsarbeit haben sich u.a. folgende Erkenntnisse ergeben:

Analyse und Verknüpfung digitaler persönlicher Daten

Muster, Zusammenhänge und Prognosen

Im Zeitalter von ***Big Data*** werden immer häufiger statistische Methoden und andere Technologien des *Data Mining* eingesetzt, um große Mengen persönlicher Daten zu analysieren und darin Muster und Zusammenhänge zu finden. Damit lassen sich Erkenntnisse über Einzelne gewinnen, die weit über die in den gesammelten Rohdaten enthaltenen Informationen hinausgehen - oder sogar **Prognosen über zukünftiges Verhalten** treffen. Die US-Supermarktkette ***Target*** konnte etwa aus einer Analyse des Einkaufsverhaltens schwangere Frauen und sogar deren Geburtstermine identifizieren - und zwar ohne dabei auf offensichtliche Käufe wie Babykleidung oder Kinderwägen angewiesen zu sein. Mehrere wissenschaftliche Studien haben belegt, dass sich aus **rudimentären Metadaten über Online-Verhalten oder *Smartphone*-Kommunikation** weitreichende Einschätzungen treffen lassen:

Was „Likes“ aussagen

- Allein aus ***Facebook-Likes*** kann mit hoher Zuverlässigkeit auf persönliche Eigenschaften wie **Geschlecht**, **Alter**, **sexuelle Orientierung**, **ethnische Zugehörigkeit**, **politische Einstellung**, **Religion**, **Beziehungsstatus** oder **Nikotin-, Alkohol-** oder **Drogenkonsum** geschlossen werden. Aus einer Analyse **anonymer Website-BesucherInnen** lassen sich deren **Geschlecht**, **Alter**, **Beruf** und **Ausbildung** abschätzen. Strukturell ähnliche Daten über

Internet-Suchanfragen, gekaufte Produkte oder musikalische Vorlieben bieten einen ähnlichen Informationsgehalt.[249]

Charakter und Emotionen

- Aus **Telefonie-Verhalten** wie etwa der Häufigkeit von Anrufen lassen sich mit einer bestimmten Wahrscheinlichkeit individuelle **Charaktereigenschaften** wie emotionale Stabilität, Extraversion, Offenheit für Neues, soziale Verträglichkeit oder Gewissenhaftigkeit berechnen - ohne auf die Kommunikationsinhalte selbst zuzugreifen. **Emotionen** wie Zuversicht, Unschlüssigkeit, Nervosität, Entspannung, Trauer oder Müdigkeit lassen sich relativ zuverlässig aus der Analyse von **Rhythmus und Dynamik des Tippens** erkennen.[250]

Zukünftiges Verhalten?

- Aus der Kenntnis **vergangener GPS-Standorte** lassen sich **zukünftige Aufenthaltsorte** prognostizieren. Wenn die Bewegungsprofile von Bekannten einbezogen werden, sind diese Vorhersagen besonders zuverlässig. Aus einer Analyse der **Verbindungen zwischen NutzerInnen** auf sozialen Netzwerken lässt sich nicht nur abschätzen, wer davon in einer romantischen Beziehung ist. Es lässt sich sogar die **Wahrscheinlichkeit einer Trennung** innerhalb der nächsten zwei Monate vorhersagen.[251]

Praktischer Einsatz in Marketing, Handel, Versicherungs-, Finanz- und Personalwirtschaft

Mit der Prognose von persönlichen Eigenschaften oder zukünftigem Verhalten aus unseren digitalen Spuren befassen sich heute nicht nur die Wissenschaft, sondern auch Geheimdienste und Unternehmen. **Werbetreibende** vermessen, segmentieren und klassifizieren ihr Publikum, steigern damit Konversionsraten und Verkäufe. Aber persönliche Daten werden inzwischen in fast allen Wirtschaftsbereichen zur **kundenspezifischen Vorhersage von Risiken, Ertragschancen oder Loyalität** eingesetzt – in Folge werden daraus Entscheidungen über einzelne Personen abgeleitet. Einige Beispiele:[252]

Viele Tippfehler – kein Kredit?

- **Bonitätsbewertung mit Online-Daten:** Das von einem ehemaligen *Google*-Mitarbeiter gegründete US-Startup *zest finance* kombiniert 70.000 Merkmale aus unterschiedlichsten Quellen, um daraus die Kreditwürdigkeit von Einzelpersonen einzuschätzen. Das Hamburger Unternehmen *Kreditech* greift dafür unter anderem auf Standort-Informationen und Daten aus sozialen Netzwerken zurück. Sogar das Surfverhalten auf der Website oder die Art, wie der Online-Kreditantrag ausgefüllt wird, fließen ein – und die Häufigkeit der Nutzung der Löschtaste.

Falscher Browser – kein Job?

- **Personalentscheidungen mit Big Data:** Die Firma *Evolv* hilft Personalabteilungen bei der Bewertung von BewerberInnen und Angestellten. Dabei fließen die Daten von inzwischen drei Millionen Personen ein – von Beschäftigungshistorie und Arbeitsleistung bis zur Anzahl der „Social Media"-Accounts oder dem benutzten Browser bei der Online-Bewerbung. Das Startup *ConnectedCube* befasst sich mit der Vorhersage der zukünftigen Leistung von Angestellten.

Unterschiedlich teure Produkte

- **Preisdiskriminierung?** Große internationale Online-Shops zeigen KonsumentInnen auf Basis von deren Online-Verhalten, Standort-Informationen, der benutzten Geräte oder Browser unterschiedliche teure Produkte an – oder gar die gleichen Produkte zu verschiedenen Preisen – mit Unterschieden bis zu 166%. Beim Online-Reisebuchungsportal *Orbitz* wurde bei Nutzung eines Mac-Computers eine Auswahl von um bis zu 13% teurerer Hotels angeboten als mit einem PC. Beim US-Bürobedarfshändler *Staples* wurde eine durchschnittliche Preisdifferenz von 8% festgestellt. KonsumentInnen haben bei derartigen Praktiken keine Chance mehr, zu verstehen, wie ihr individueller Preis oder die Auswahl der

249 Siehe Kapitel 3.2.2 und 3.2.4
250 Siehe Kapitel 3.2.3 und 3.2.5
251 Siehe Kapitel 3.2.6 und 3.2.7
252 Siehe Kapitel 3.3 und 3.4

ihnen angebotenen Produkte zustande kommen.

Achtung beim Einkauf oder beim Spielen

- **Krankheitsprognosen aus Konsumverhalten:** Die große US-Versicherung *Aviva* beschäftigt sich mit der Prognose von Risiken für Krankheiten wie Diabetes, hohem Blutdruck oder Depression allein aus Daten über Konsumverhalten, Lebensstil oder Einkommen.
- **Emotionale Manipulation?** Das Werbeunternehmen *MediaBrix* analysiert die Emotionen von Online-SpielerInnen, spricht diese gezielt und individuell in ganz bestimmten Momenten zwischen Begeisterung und Frustration an und konnte damit die Effektivität der Werbung im Web um 15% und bei mobilen *Apps* sogar um 30% steigern.

Datenhungrige Geräte und Plattformen

Smartphones und die darauf installierten *Apps* sind eines der größten Einfallstore für Unternehmen, die persönliche Daten über NutzerInnen sammeln. Auto-Versicherungstarife auf Basis von Rundum-Überwachung könnten zum Vorbild für andere Bereiche werden. Die von Fitness-Trackern, *Smartwatches* und *Apps* gemessenen Daten über Körper und Gesundheit haben großes kommerzielles Potenzial. Im *Internet der Dinge* wird die Überwachung durch vernetzte Sensoren omnipräsent.

Spione in der Hosentasche?

- ***Smartphones*** ermöglichen mit ihren unzähligen Sensoren und den darauf gespeicherten Daten sehr weitgehende Einblicke in Persönlichkeit und Alltag ihrer BesitzerInnen. 71% der kostenlosen *Android*-Apps und 32% der kostenlosen *iOS*-Apps übertragen persönliche Daten an Werbenetzwerke, mehr als die Hälfte greifen auf sensible Informationen wie Standort-Daten zu. Nach einer Untersuchung von 26 Datenschutzbehörden aus 19 Ländern greifen 31% von 1200 populären *Apps* auf Daten dazu, ohne dass dies für die eigentliche Funktion der *App* notwendig wäre. 59% der *Apps* werden als bedenklich eingestuft, da sie die NutzerInnen nicht ausreichend darüber informieren, welche Daten genutzt und weitergegeben werden.[253]

Günstigere Versicherung

- **Überwachungsboxen im Auto** zeichnen rund um die Uhr das Fahrverhalten auf und übertragen Position, Geschwindigkeit und Beschleunigungswerte an Versicherungen, die die Höhe der Prämienzahlung von den gemessenen Daten abhängig machen: In Italien, Frankreich, Spanien, Großbritannien und den USA ist dieses Prinzip schon etabliert, für 2020 werden global 100 Millionen derartige Polizzen erwartet. In Deutschland existiert ein erstes Angebot der *Sparkassen-DirektVersicherung*. Wer dabei zu viel in der Nacht oder in der Stadt fährt, oder zu oft stark beschleunigt oder bremst, riskiert einen Verlust des Prämienrabatts von 5%.[254]

Weitergabe von Gesundheitsdaten

- **Fitness-Tracker und *Smartwatches*:** Tragbare Geräte und *Apps* zur Auswertung von Schritten, Puls, Schlaf und vielen anderen Körperfunktionen sind inzwischen ein Milliarden-Geschäft. Während die NutzerInnen mit Spielmechaniken, Anreizen und Belohnungen dazu motiviert werden, diese *Wearables* möglichst oft zu nutzen, arbeiten die Unternehmen an Geschäftsmodellen zur kommerziellen Verwertung der erfassten Daten. Der Marktführer *Fitbit* wirbt öffentlich mit Angeboten für Versicherungen und arbeitet international bereits mit vielen großen Unternehmen im Rahmen betrieblicher Gesundheitsprogramme zusammen. Bei der US-Firma *Appirio* stellen etwa 1.000 Angestellte freiwillig ihre mit *Fitbit* gemessenen Gesundheitsdaten zur Verfügung, die Firma konnte dadurch eine jährliche Ermäßigung von 300.000 Dollar mit der betrieblichen Krankenversicherung ausverhandeln. Angestellte des Ölkonzerns *BP* werden dazu angehalten, mit *Fitbit* eine Million Schritte pro Jahr zu erreichen – ein Mitarbeiter ersparte sich dadurch 1.200 Dollar bei der jährlichen Krankenversi-

253 Siehe Kapitel 4.1
254 Siehe Kapitel 4.3

cherungsprämie. Dies ist ein durchaus starker Anreiz und bedeutet umgekehrt: Wer nicht teilgenommen oder das „spielerische" Ziel nicht erreicht hat, wird bestraft und bezahlt spürbar mehr. Große US-Versicherer haben bereits Programme gestartet, die *Wearables* integrieren und bei denen KonsumentInnen bei Erreichen bestimmter Fitness-Ziele kleine Belohnungen wie Einkaufsgutscheine oder Kinotickets erhalten können. Es ist wahrscheinlich nur mehr eine Frage der Zeit, bis auch KonsumentInnen in den USA direkte Rabatte auf Versicherungsprämien erhalten – oder gar Strafen bei Nicht-Erreichen der Fitness-Ziele.[255]

Vernetzte Sensoren im Alltag

- **Allgegenwärtige Überwachung im *Internet der Dinge*?** Immer mehr Alltagsgegenstände sind mit kleinen vernetzten Computer und Sensoren ausgerüstet. Neben den in *Smartphones* schon üblichen Sensoren vermessen *Wearables* nicht mehr nur Schritte, Puls oder Schlaf, sondern auch Atmung, Hautwiderstand, Blutdruck oder Blutzucker - und verfügen über Barometer, Temperatur- oder Luftfeuchtigkeitssensoren. *E-Book-Reader* zeichnen detaillierte Informationen zum Leseverhalten auf, vernetzte TV-Geräte versenden Daten über das Fernsehverhalten. Vernetzte Autos, Stromzähler, Thermostaten, Brandmelder, Kühlschränke oder Badewannen liefern bald umfangreiche Daten über unser Alltagsverhalten. Dabei überwachen die NutzerInnen nicht nur sich selbst, sondern auch andere - etwa ihre Kinder oder ihre Angestellten, die entweder Geräte mit Sensoren mit sich tragen oder sich an Orten bewegen, die mit Sensoren ausgestattet sind. Datenbrillen und *Wearables* zur digitalen Vermessung von Körper, Gesundheit, Verhalten und Umgebung werden unauffälliger - etwa in Form von Pulssensoren in biometrischen Kopfhörern, Temperatur- und Feuchtigkeitssensoren in elektronischen Tattoos oder durch mit Sensoren ausgestatteten Ringen, Socken, T-Shirts, Büstenhalter, Zahnbürsten oder Gabeln. Viele ExpertInnen erwarten, dass Anreize zur Verhaltensänderung zum zentralen Treiber für das *Internet der Dinge* werden - beispielsweise Anreize zum Kauf eines Produkts, zur Anregung von gesünderen oder sichereren Lebensweisen oder von bestimmten Arbeitsweisen. Dies könnte laut ExpertInnen zu massiven Auswirkungen auf die Möglichkeit führen, das eigene Leben zu kontrollieren.[256]

Das Geschäft mit den persönlichen Daten

Sowohl im deutschen Sprachraum als auch international existiert eine Vielzahl von Unternehmen, die sich in der einen oder anderen Weise dem Handel mit persönlichen Daten verschrieben haben:

Adressen von kirchlichen Verlagen bis Erotik

- **Daten- und Adresshandelsfirmen im deutschen Sprachraum** handeln mit Adressen und Persönlichkeitsprofilen über viele Millionen Menschen. Marktführer sind *Bertelsmann*, *Otto* und die *deutsche Post*. Das *Bertelsmann*-Tochterunternehmen *AZ Direkt* verkauft Daten über ältere oder verschuldete Menschen, Spendenwillige oder „risikobereite Individualisten" - sowie Adressen aus so unterschiedlichen Quellen wie der Erotik-Versandhandelsmarke *Beate Uhse*, kirchlichen Verlagen oder der Wochenzeitung *Die Zeit*. Die Auswahl der gekauften Daten kann fein abgestimmt werden - geworben wird mit „mehr als 600 adressqualifizierende Profilinformationen zum Beispiel zu Soziodemografie, Psychografie, Konsumeigenschaften, Lebensphasen".[257]

Von Negativlisten zu komplexen Scoring-Modellen

- **Wirtschaftsauskunfteien im deutschen Sprachraum** bieten Bonitätsbewertung von Privatpersonen und andere Dienstleistungen an. Einfache Negativlisten wurden inzwischen von komplexen Scoring-Modellen abgelöst, die viele Lebensumstände in die Berechnung der Kreditwürdigkeit einbeziehen. Die Berechnungsmethoden sind oft fehleranfällig und in-

255 Siehe Kapitel 4.2
256 Siehe Kapitel 4.4
257 Siehe Kapitel 5.1

transparent, die VerbraucherInnen schlecht informiert. Die dominanten Unternehmen und deren Tochterfirmen sind oft gleichzeitig in den Bereichen Direktmarketing, Daten- und Adresshandel aktiv. Die auch in Österreich tätige *Bertelsmann*-Tochterfirma *arvato* wickelt etwa mit ihren Tochterfirmen nicht nur Bonitätsprüfungen, Scoring, Inkasso und Finanzdienstleistungen ab, sondern betreibt auch Kundenclubs und Bonusprogramme für große Unternehmen, Präventionsprogramme im Gesundheitsbereich sowie das „Hinweis- und Informationssystem der deutschen Versicherungswirtschaft". Die Tochterfirma *arvato infoscore* hat „Negativinformationen" zu 7,8 Millionen Personen gespeichert. Mit dem System *infoRate+* kann laut Website zur „Bewertung eines Konsumenten auf vielfältigste Datenquellen zugegriffen" werden - Unternehmen könnten damit „sämtliche vorhandenen internen und externen Daten verdichten und integrieren". Ein weiteres angebotenes *Scoring*-Produkt wird mit folgendem Satz beworben: „Kunden mit hohem Ertragspotenzial sollen gewonnen, Kunden mit hohem Risiko von Anfang an gemieden werden".[258]

Acxiom: Daten über 700 Millionen Menschen

- **Internationale Player im Geschäft mit den persönlichen Daten** in den USA – sogenannte *Data Broker* - verfügen über umfangreiche Dossiers über die gesamte Bevölkerung, sammeln laut der US-amerikanischen *Federal Trade Commission* Daten über KonsumentInnen aus umfassenden Online- und Offline-Quellen und speichern diese teils unbefristet – und zwar "größtenteils ohne das Wissen der Konsumenten". Sie sammeln enorme Mengen von Daten – von Zahlungsverhalten und Zeitschriften-Abos über Aktivitäten in sozialen Medien bis zu religiösen und politischen Zugehörigkeiten – machen Schlussfolgerungen über ethnische Zugehörigkeit, Einkommen oder Gesundheit und verkaufen Informationen an Handel, Politik, Versicherungen oder Personalabteilungen. Die US-Firma *Acxiom* verfügt etwa über umfangreiche Dossiers mit bis zu 3.000 einzelnen Eigenschaften von etwa 700 Millionen Menschen – von Ausbildung, Wohnen, Beschäftigung, Finanzen und Eigentum bis zu Wahlverhalten, „Bedürfnissen" und „Interessen" im Bereich Gesundheit oder der „Neigung zum Glücksspiel". Das Unternehmen betreibt 15.000 Kundendatenbanken von globalen Top-Unternehmen, kooperiert mit *Google*, *Facebook* und *Twitter* und hat seit dem Kauf des Online-Spezialisten *Liveramp* laut Eigenangabe drei Milliarden Kundendatensätze „ins Web gebracht". *Acxiom* ist auch in Deutschland tätig und besitzt laut der Wochenzeitung *Die Zeit* Daten über 44 Millionen Deutsche.[259]

Datalogix, Lexis Nexis und Recorded Future

- **Weitere Beispiele für internationale „Data Broker":** Das Unternehmen *Datalogix* verfügt über mehr als eine Trillion Transaktionsdaten von KonsumentInnen in den USA und vergleicht im Rahmen einer Partnerschaft mit *Facebook*, wie oft NutzerInnen online Werbung für bestimmte Produkte sehen - und die entsprechenden Käufe dann in einem Geschäft durchführen. Die Firma *Lexis Nexis* gibt an, Daten über 500 Millionen KonsumentInnen zu besitzen und bietet „Risikomanagement-Lösungen" in den Bereichen Versicherung, Handel oder für den Gesundheitssektor an. Angeboten werden unter anderem Daten über die Kreditwürdigkeit, Hintergrund-Überprüfungen von ArbeitnehmerInnen oder Informationen über „Problem-Mieter". Darüber hinaus werden biometrische Services vom Fingerabdruck bis zur Stimmerkennung oder zur Erkennung von „Risiken und Bedrohungen" in sozialen Medien angeboten. Das Unternehmen *Recorded Future* erfasst Daten über Personen von fast 600.000 Websites in sieben Sprachen, nutzt diese Informationen, um deren zukünftiges Verhalten vorherzusagen und arbeitet sowohl für Unternehmen als auch für Militär und Geheimdienste - seit 2009 sind unter anderem *Google* und *In-Q-Tel* und damit indirekt der US-Geheimdienst *CIA* an *Recorded Future* beteiligt.[260]

---

258 Siehe Kapitel 5.2
259 Siehe Kapitel 5.3
260 Siehe Kapitel 5.3

Zugriff auf 1,4 Milliarden Geräte

- **Tausende Firmen in den Bereichen Online-Tracking, Analyse und Werbung** identifizieren NutzerInnen über Websites, *Apps* und Geräte hinweg und sammeln gewaltige Mengen an persönlichen Informationen. Beim Aufruf beinahe aller populären Websites wird jeder einzelne Klick an mehrere Dritt-Unternehmen übertragen, ebenso bei vielen Smartphone-*Apps*. Die Analyse- und Werbeplattform *Flurry* ist global auf 1,4 Milliarden Smartphones und Tablets installiert und zeichnet die Nutzungsaktivitäten in 540.000 *Apps* auf. *Flurry* ermöglicht Werbetreibenden eine gezielte Ansprache nach Geschlecht, Alter und Interessen - und sortiert NutzerInnen in Kategorien wie Hardcore-SpielerInnen, frischgebackene Mütter oder nach ihrer sexuellen Orientierung. Durch eine Kooperation mit der Marktforschungsfirma *Research Now* stehen seit kurzem weitere 350 „Profil-Attribute" über Demographie, Interessen und Lifestyle zur Verfügung.[261]

Gesellschaftliche Auswirkungen von kommerzieller digitaler Überwachung[262]

Permanente Sortierung der Bevölkerung

Durch die beschriebenen Entwicklungen und Praktiken wird klar, dass eine Art von **Überwachungsgesellschaft** Realität geworden ist, in der die Bevölkerung ständig auf Basis persönlicher Daten **klassifiziert und sortiert** wird. KonsumentInnen können oft **nicht mehr nachvollziehen**, welche Daten über sie und ihr Verhalten von Unternehmen digital erfasst und gespeichert werden, wie diese Daten verarbeitet werden, an wen sie weitergegeben oder verkauft werden, welche Schlüsse daraus gezogen werden und welche Entscheidungen auf Basis dieser Schlüsse über sie gefällt werden. Persönliche Daten werden zunehmend **in völlig anderen Bereichen eingesetzt** als die ursprünglichen Verwendungszwecke bei deren Erfassung. Außerdem besteht überall, wo große Datenmengen gespeichert werden, das Risiko von **Datenmissbrauch und -verlust**. Dadurch entstehen große Risiken für Einzelne – von Belästigung und Stalking bis Identitätsdiebstahl und Cyber-Kriminalität.

Auswirkungen auf lebensentscheidende Fragen

Wenn Unternehmen Kriterien wie Geschlecht, Alter, ethnische oder religiöse Zugehörigkeit, Armut oder den Gesundheitszustand in ihre Entscheidungen mit einbeziehen, besteht die Gefahr von **Diskriminierung oder Ausschluss** ganzer Bevölkerungsgruppen. Die Chancen und Wahlmöglichkeiten von Einzelnen können dadurch eingeschränkt werden – von Preisdiskriminierung und der der Frage, welche Angebote jemand bekommt bis zu **lebensentscheidenden Fragen** in den Bereichen Finanzen, Gesundheit, Versicherung oder Arbeit. Sogar die *Federal Trade Commission* befürchtet, dass für KonsumentInnen mit „riskanteren" Verhaltensweisen in Zukunft höhere Versicherungsprämien anfallen könnten. Michael Fertik diagnostiziert im *Scientific American*, dass durch individuelle Preise und personalisierte Angebote schon jetzt die „Reichen" ein „anderes Internet als die Armen" sehen würden.

Wer sich falsch verhält…

Abgesehen von **Fehlern bei der Erfassung** der gesammelten Daten können Fehler in den Prognosemodellen und damit **falsche Schlussfolgerungen** massive negative Auswirkungen auf Einzelne haben. Wer beispielsweise die falschen Personen kennt, im falschen Bezirk wohnt oder sich in der *Smartphone-App* „falsch" verhält, wird in einer bestimmten Art und Weise klassifiziert und muss die Konsequenzen tragen, ohne Einfluss darauf zu haben. Auch eine **Verweigerung der Teilnahme** kann Konsequenzen haben: Wenn keine oder zu wenige Daten über eine Person vorhanden sind, schätzt ein Unternehmen das Risiko für eine Kundenbeziehung unter Umständen prinzipiell als zu hoch ein. Wenn Versicherungsunternehmen die Risikoabschätzung von Lebensgewohnheiten und Verhaltensweisen abhängig machen, wird außerdem **Risiko individualisiert**. Der Netz-Theoretiker Evgeny Morozov warnt vor einer mit der „Umweltkatastrophe" vergleichbaren „Datenkatastrophe", die uns in einer Welt erwartet, in der persönliche Daten

261 Siehe Kapitel 5.4
262 Siehe Kapitel 6

wie Kaffee oder jede andere Ware gehandelt werden“.

Handlungsempfehlungen für Politik, Öffentlichkeit, Unternehmen und BürgerInnen[263]

Was tun?

Der digitale Wandel schreitet auf allen gesellschaftlichen Ebenen schreiten mit einer Geschwindigkeit voran, der viele EntscheidungsträgerInnen mit einer gewissen Ohnmacht und Ratlosigkeit gegenüberstehen. Allgegenwärtige digitale Überwachung könnte künftig **drastische Auswirkungen auf Gesellschaft, Demokratie und die Autonomie des Einzelnen** haben. Gleichzeitig bieten digitale Kommunikationstechnologien große Chancen und Möglichkeiten in vielen gesellschaftlichen Bereichen. Um die möglichen negativen Auswirkungen zu minimieren, wird unter anderem folgendes empfohlen:

- **Schaffung von Transparenz** über die Praktiken von Unternehmen – durch Forschung, Öffentlichkeit und Regulierung.
- **Unterstützung von dezentralen Technologien**, die mehr Kontrolle über persönliche Daten einräumen – auf allen Ebenen der Forschungs-, Förderungs- und Vergabepraxis.
- **Stärkung von digitaler Zivilgesellschaft und kritischem Diskurs** über Chancen, Risiken, Machtungleichgewichte und Lösungsmöglichkeiten.
- **Stärkung von digitaler Kompetenz** und von Wissen über den Umgang mit den eigenen persönlichen Daten.
- Maximale Aufmerksamkeit auf eine gute und trotzdem zügige Ausgestaltung der **europäischen Datenschutzverordnung**.

263 Siehe Kapitel 6.3.

Literatur

ARGE Daten (2006): Indirekt personenbezogene Daten - Sind Einschränkungen im DSG 2000 europarechtskonform? 25.10.2006. Online: http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=75776hwg

Agrawal, Rakesh; Srikant, Ramakrishnan (2000): Privacy-Preserving Data Mining. ACM SIGMOD Int'l Conf. on Management of Data, Dallas, May 2000. Online: http://rakesh.agrawal-family.com/papers/sigmod00ppdm.pdf

Albrecht, Jan Philipp (2014): Finger weg von unseren Daten! Wie wir entmündigt und ausgenommen werden. Droemer Knaur.

Alter, Alexandra (2012): Your E-Book Is Reading You. The Wall Street Journal, 19.07.2012. Online: http://online.wsj.com/news/articles/SB10001424052702304870304577490950051438304

Appthority (2014): App Reputation Report. Summer 2014. Whitepaper. Online: https://www.appthority.com/app-reputation-report/report/AppReputationReportSummer14.pdf

Boyd Dana; Crawford, Kate (2012): Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon, Information, Communication & Society 15:5, S.662-679. Online: http://www.tandfonline.com/doi/abs/10.1080/.VB8Tz_l_uCk

CIP/Oracle (2013): Talent analytics and big data – the challenge for HR. Research Report, November 2013. Online http://www.oracle.com/us/products/applications/human-capital-management/talent-analytics-and-big-data-2063584.pdf

Deterding, Sebastian; Khaled, Rilla; Nacke, Lennart; Dixon, Dan (2011): Gamification: Toward a Definition, Proc. Workshop on Gamification at the ACM Intl. Conf. on Human Factors in Computing Systems (CHI).

De Zwart, Melissa; Humphreys, Sal; Van Dissel, Beatrix (2014). Surveillance, big data and democracy: lessons for Australia from the US and UK, UNSW Law Journal. Online: http://www.unswlawjournal.unsw.edu.au/sites/default/files/final_t3_de_zwart_humphreys_and_van_dissel.pdf

Dobusch Leonhard (2014): Digitale Zivilgesellschaft in Deutschland. Stand und Perspektiven 2014. Freie Universität Berlin, Fachbereich Wirtschaftswissenschaft, Diskussionsbeiträge. Online: http://edocs.fu-berlin.de/docs/servlets/MCRFileNodeServlet/FUDOCS_derivate_000000003411/discpaper2014_7.pdf

Duhigg, Charles (2012): Die Macht der Gewohnheit. Berlin Verlag.

Dumortier, Franck (2009). Facebook and Risks of "De-contextualization" of Information. In: Monograph "5th Internet, Law and Politics Congress. The Pros and Cons of Social Networks", Universitat Oberta de Catalunya. Online: http://journals.uoc.edu/index.php/idp/article/viewFile/n9_dumortier/n9_dumortier_eng

Eggers, Dave (2014): Der Circle. Aus dem amerikanischen Englisch von Ulrike Wasel und Klaus Timmermann. Kiepenheuer & Witsch, Köln 2014.

Enck, W.; Gilbert, P.; Chun, B.; Cox, L.; Jung, J.; Mc-Daniel, P.; Sheth, A. (2010): TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In Proc. of USENIX Symposium on Operating Systems Design and Implementation (OSDI). Online: http://static.usenix.org/event/osdi10/tech/full_papers/Enck.pdf

Fertik, Michael (2013): The Rich See a Different Internet Than the Poor. Ninety-nine percent of us live on the wrong side of a one-way mirror. Scientific American, 14.01.2013. Abgerufen am 19.09.2014 von http://www.scientificamerican.com/article/rich-see-different-internet-than-the-poor/

FTC, US Federal Trade Commission (2014): Data Brokers. A Call for Transparency and Accountability. Online: http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Gabriel, Peter; Gaßner, Katrin; Lange, Sebastian (2010): Das Internet der Dinge – Basis für die IKT-Infrastruktur von morgen. Anwendungen, Akteure und politische Handlungsfelder. Institut für Innovation und Technik, Berlin.

Gandy, Oscar (2006): Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment. In: Haggerty, K., Ericson, R. (2006) The New Politics of Surveillance and Visibility, Toronto, University of Toronto Press.

GAO, United States Government Accountability Office (2006): Personal Information. Agency and Reseller Adherence to Key Privacy Principles. GAO-06-421, April 2006. Online: http://www.gao.gov/new.items/d06421.pdf

Han, Jiawei; Kamber, Micheline; Pei, Jian (2011): Data Mining: Concepts and Techniques, 3rd ed. The Morgan Kaufmann Series in Data Management Systems.

Hansen, Marit (2012): Überwachungstechnologien. In: Schmidt, Jan-Hinrik; Weichert, Thilo (Hrsg.) (2012): Datenschutz. Grundlagen, Entwicklungen und Kontroversen, 1. Auflage, Bundeszentrale für politische Bildung, Bonn, S. 23-32. Online: http://edoc.hu-berlin.de/miscellanies/steinmueller-40657/45/PDF/45.pdf

Hardest, Larry (2013): How hard is it to 'de-anonymize' cellphone data? MIT News, 27.03.2013. Online:

http://newsoffice.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data

Ito, Aki (2013): Hiring in the Age of Big Data. Bloomberg Businessweek, 24.10.2013. Abgerufen am 14.09.2014 von http://www.businessweek.com/articles/2013-10-24/new-way-to-assess-job-applicants-online-games-and-quizzes

Korczak, Dieter; Wilken, Michael (2009): Verbraucherinformation Scoring. Bericht im Auftrag des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz. München. Online: http://www.bmelv.de/cae/servlet/contentblob/638114/publicationFile/36026/Scoring.pdf

Lewinski, Kai von (2012): Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive. In: Schmidt, Jan-Hinrik; Weichert, Thilo Hrsg.: Datenschutz. Grundlagen, Entwicklungen und Kontroversen, 1. Auflage, Bundeszentrale für politische Bildung, Bonn, S. 23-32. Online: http://edoc.hu-berlin.de/miscellanies/steinmueller-40657/45/PDF/45.pdf

Lyon, David (1994): The Electronic Eye: The Rise of Surveillance Society, Minneapolis, University of Minnesota Press.

Lyon, David (2003) Surveillance as social sorting: Computer codes and mobile bodies. In: Lyon, D. (Hrsg.): Surveillance as social sorting: Privacy, risk, and digital discrimination. Routledge, London, New York.

Lyon, David (2007): Surveillance Studies: An Overview. Cambridge: Polity Press.

Manovich, Lev (2011) Trending: the promises and the challenges of big social data. In: Debates in the Digital Humanities, ed. M. K. Gold, The University of Minnesota Press, Minneapolis, MN. Online: http://manovich.net/content/04-projects/065-trending-the-promises-and-the-challenges-of-big-social-data/64-article-2011.pdf

Manyika, James; Chui, Michael; Brown, Brad; Bughin, Jacques; Dobbs, Richard; Roxburgh, Charles; Hung Byers, Angela (2011): Big data: The next frontier for innovation, competition, and productivity, McKinsey&Company, McKinsey Global Institute. Online: http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data_full_report.ashx

Mattern, Friedemann (2005): Die technische Basis für das Internet der Dinge. In: Elgar Fleisch, Friedemann Mattern (Hrsg.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis. Springer-Verlag, pp. 39-66. Online: http://www.vs.inf.ethz.ch/publ/papers/internetdinge.pdf

Mattioli, Dana (2012): On Orbitz, Mac Users Steered to Pricier Hotels. Wall Street Journal, 23.08.2012. Abgerufen am 20.09.2014 von http://online.wsj.com/news/articles/SB10001424052702304458604577488822667325882

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

Mikians, Jakub; Gyarmati, László; Erramilli, Vijay; Laoutaris, Nikolaos (2012): Detecting price and search discrimination on the internet. In Proceedings of the 11th ACM Workshop on Hot Topics in Networks (HotNets-XI). ACM, New York, NY, USA, 79-84. Online: http://conferences.sigcomm.org/hotnets/2012/papers/hotnets12-final94.pdf

Morozov, Evgeny (2013): Der Preis der Heuchelei. Ideologie des Datenkonsums. Frankfurter Allgemeine Zeitung, 24.07.2013. Online: http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/ideologie-des-datenkonsums-der-preis-der-heuchelei-12292822.html

Office of the Privacy Commissioner of Canada (2014): Global Privacy Enforcement Network (GPEN) Privacy Sweep. Online: https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp

Palmås, Karl (2011): Predicting What You'll Do Tomorrow: Panspectric Surveillance and the Contemporary Corporation. In: Surveillance & Society, Vol 8, No 3. Online: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/4168

Peck, D. (2013): They're Watching You at Work. What happens when Big Data meets human resources? The emerging practice of "people analytics" is already transforming how employers hire, fire, and promote. The Atlantic, 20.11.2013. Online: http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/

Pew Research Center (2014): The Internet of Things Will Thrive by 2025. Mai 2014. Online: http://www.pewinternet.org/2014/05/14/internet-of-things

Pfitzmann, Andreas; Hansen, Marit (2010): A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. Version 0.34, August 2010. Online: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Pohle, Jörg (2014). Die immer noch aktuellen Grundfragen des Datenschutzes. In: Garstka, H., Coy, W. (Hrsg.): Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis. (pp. 45-58). Berlin: Helmholtz-Zentrum für Kulturtechnik, Humboldt-Universität zu Berlin.

Richards, Neil (2013): The Dangers of Surveillance. Harvard Law Review 126, 1934, 1953. Online: http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der

Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Online: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:31995L0046

Rössler, Beate (2001), Der Wert des Privaten, ed. Suhrkamp Taschenbuch (Frankfurt am Main).

Rothmann, Robert; Sterbik-Lamina, Jaro; Peissl, Walter (2014) Credit Scoring in Österreich. Bericht-Nr. ITA-PB A66; Institut für Technikfolgen-Abschätzung (ITA): Wien; im Auftrag von: Bundesarbeitskammer. Online: http://epub.oeaw.ac.at/ita/ita-projektberichte/a66.pdf

Rothmann, Robert; Sterbik-Lamina, Jaro; Peissl, Walter; Čas, Johann (2012) Aktuelle Fragen der Geodaten-Nutzung auf mobilen Geräten – Endbericht. Bericht-Nr. ITA-PB A63; Institut für Technikfolgen-Abschätzung (ITA): Wien; im Auftrag von: Österreichische Bundesarbeitskammer. Online: http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a63.pdf

Satariano, Adam (2014): Wear This Device So the Boss Knows You're Losing Weight. Bloomberg. Online: http://www.bloomberg.com/news/2014-08-21/wear-this-device-so-the-boss-knows-you-re-losing-weight.html

Schrems, Max (2014): Kämpf um deine Daten. Edition a, Wien.

Scism, Leslie; Maremont, Mark (2010): Insurers Test Data Profiles to Identify Risky Clients. The Wall Street Journal, 19.11.2010. Online: http://online.wsj.com/articles/SB10001424052748704648604575620750998072986

Singer, Natasha (2012): You for Sale. Mapping, and Sharing, the Consumer Genome. New York Times, 16.06.2012. Abgerufen am 10.07.2014 von http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html

Sterbik-Lamina, Jaro; Peissl, Walter; Cas, Johann (2009): Privatsphäre 2.0 (Beeinträchtigung der Privatsphäre in Österreich; Neue Herausforderungen für den Datenschutz). Bericht-Nr. A53; Institut für Technikfolgen-Abschätzung (ITA): Wien. Online: http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a53.pdf

Tanner, Adam (2014): Different Customers, Different Prices, Thanks To Big Data. Forbes, 26.03.2014. Abgerufen am 20.09.2014 von http://www.forbes.com/sites/adamtanner/2014/03/26/different-customers-different-prices-thanks-to-big-data/

Thurm, S.; Kane, Y. (2010): Your Apps Are Watching You, Wall Street Journal. Online: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html, In: What They Know. Online: http://blogs.wsj.com/wtk-mobile/

Tretter, Hannes (2010): Aktuelle datenschutzrechtliche Herausforderungen in Österreich. In: Die Zukunft, Ausgabe 1/2010. Online: http://diezukunft.at/?p=1070

Urban, Jennifer M.; Hoofnagle, Chris Jay; Li, Su: Mobile Phones and Privacy. Berkeley Consumer Privacy Survey, BCLT Research Paper, 11.07.2012. Online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405

Valentino-Devries, Jennifer; Singer-Vine, Jeremy; Soltani, Ashkan (2012): Websites Vary Prices, Deals Based on Users' Information. Wall Street Journal. Abgerufen am 20.09.2014 von http://online.wsj.com/news/articles/SB10001424127887323777204578189391813881534

Wall Street Journal (2010): What They Know. Online: http://blogs.wsj.com/wtk

WEF, World Economic Forum (2012): Rethinking Personal Data. Strengthening Trust. Online: http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf

Weichert, Thilo (2013): Big Data und Datenschutz. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. Online: https://www.datenschutzzentrum.de/bigdata/20130318-bigdata-und-datenschutz.pdf

Weiser, Mark (1991): The Computer for the 21st Century. Scientific American, September 1991. Entwurfsversion online unter: http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html

@stefanwehrmeyer, @annabelchurch, @pudo (2014): We used to read the newspaper, now the news reads us. Abgerufen am 18.09.2014 von http://newsreadsus.okfn.de

Weitere Texte und Zeitungsartikel:

Bergen, Mark (2014): Flurry Launches Service to Track Mobile App Users, Offline The Analytics Firm Partners With Research Now, As the Race to Target Inside Apps Picks Up. Advertising Age, 24.03.2014. Abgerufen am 18.09.2014 von: http://adage.com/article/digital/flurry-research-build-mobile-app-advertising-database/292287/

Dwoskin, Elizabeth (2014): Data Broker Acxiom Moves to Tie Physical World to Online Data. Wall Street Journal, 14.05.2014. Abgerufen am 10.04.2014 von: http://blogs.wsj.com/digits/2014/05/14/data-broker-acxiom-moves-to-tie-physical-world-to-online-data

Friedrichs, Julia: Selbstoptimierung. Das tollere Ich. Zeit Magazin, 12.08.2013. Abgerufen am 04.07.2014 von: http://www.zeit.de/2013/33/selbstoptimierung-leistungssteigerung-apps

Hardy, Quentin (2012): Just the Facts. Yes, All of Them. New York Times, 25.03.2012. Abgerufen am 14.09.2014 von: http://www.nytimes.com/2012/03/25/business/factuals-gil-elbaz-wants-to-gather-the-data-universe.html

Harford, Tim (2014): Big data: are we making a big mistake? Financial Times, 28.03.2014. Abgerufen am 14.09.2014 von: http://www.ft.com/intl/cms/s/2/21a6e7d8-b479-11e3-a09a-00144feabdc0.html#axzz3DK9lcAdI

Heider, Jens; Khayari, Rachid El (2012), Geht Ihr Smartphone fremd? Datenschutz und Datensicherheit, 36/3/2012, S. 155-60. Abgerufen am 07.07.2014 von: https://www.sit.fraunhofer.de/fileadmin/dokumente/artikel/DuD-Artikel_geht_ihr_Smartphone_fremd.pdf

Hill, Kashmir (2014): 10 Other Facebook Experiments On Users, Rated On A Highly-Scientific WTF Scale. Forbes, 10.07.2014. Abgerufen am 14.09.2014 von: http://www.forbes.com/sites/kashmirhill/2014/07/10/facebook-experiments-on-users/

Kaye, Kate (2014): Acxiom Acquires LiveRamp to Boost Offline-to-Online Data Capability. Advertising Age, 14.05.2014. Abgerufen am 10.07.2014 von: http://adage.com/article/datadriven-marketing/acxiom-buys-liveramp-offline-online-data-capability/293212/

Kollaten Venne, Patrick; Eikenberg, Ronald; Schmidt; Jürgen (2012), Selbstbedienungsladen Smartphone, c't, Heft 7/2012, S. 114.

Laughlin, Andrew (2014): Smart TV spying – are you watching TV, or is it watching you? Which? Magazine, 20.08.2014. Abgerufen am 20.09.2014 von: http://blogs.which.co.uk/technology/tvs/smart-tv-spying-weve-investigated

Maass, Peter; Rajagopalan, Megha (2012): That's No Phone. That's My Tracker. New York Times, 13.07.2012. Abgerufen am 10.07.2014 von: http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html

Marwede-Dengg, Claudia (2013): Versicherungen: Unter Verdacht. Euro am Sonntag, 07.09.2013. Abgerufen am 10.07.2014 von: http://www.finanzen.net/nachricht/private-finanzen/Auskunftei-fuer-Versicherer-Versicherungen-Unter-Verdacht-2630684

Mclaughlin, Catriona (2013): Acxiom. Die Besserwisser. Die Zeit, 05.07.2013. Abgerufen am 10.07.2014 von: http://www.zeit.de/2013/28/acxiom/komplettansicht

Myslewski, Rik: The Internet of Things helps insurance firms reward, punish. The Register, 24.05.2014. Abgerufen am 19.09.2014 von: http://www.theregister.co.uk/2014/05/23/the_internet_of_things_helps_insurance_firms_reward_punish/

Olson, Parmy (2013): Meet The Company That Tracks More Phones Than Google Or Facebook. Forbes, 30.10.2013. Abgerufen am 18.09.2014 von: http://www.forbes.com/sites/parmyolson/2013/10/30/meet-the-company-that-tracks-more-phones-than-google-or-facebook/

Olson, Parmy (2014): The Quantified Other: Nest And Fitbit Chase A Lucrative Side Business. Forbes, 05.05.2014. Abgerufen am 05.07.2014 von: http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest-and-fitbit-chase-a-lucrative-side-business

Olson, Parmy (2014b): Wearable Tech Is Plugging Into Health Insurance. Forbes, 19.06.2014. Abgerufen am 05.07.2014 von: http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/

Peck, Don (2014): They're Watching You at Work. What happens when Big Data meets human resources? The emerging practice of "people analytics" is already transforming how employers hire, fire, and promote. The Atlantic, 20.11.2013. Abgerufen am 19.09.2014 von: http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/

Schulz, Thomas; Müller, Martin; Rosenbach, Marcel (2013): Die Daten-Bank. Spiegel, 14.05.2013. Abgerufen am 14.09.2014 von: http://www.spiegel.de/netzwelt/netzpolitik/big-data-daten-bank-a-899538.html

Simonite, Tom (2013): Ads Could Soon Know If You're an Introvert (on Twitter). MIT Technology Review, 08.11.2013. Abgerufen am 14.09.2013 von: http://www.technologyreview.com/news/520671/ads-could-soon-know-if-youre-an-introvert-on-twitter/

Talbot, David (2012): A Phone that Knows Where You're Going. MIT Technology Review, 09.07.2012. Abgerufen am 14.09.2014 von: http://www.technologyreview.com/news/428441/a-phone-that-knows-where-youre-going/

Wiesmüller, Max (2014): Notrufsystem eCall ist ab 2015 Pflicht in Autos. Die Welt, 17.09.2014. Abgerufen am 20.09.2014 von: http://www.welt.de/wirtschaft/webwelt/article132332877/Notrufsystem-eCall-ist-ab-2015-Pflicht-in-Autos.html

Wolf, Gary: The Data-Driven Life. New York Times, 02.05.2010. Abgerufen am 04.07.2014 von: http://www.nytimes.com/2010/05/02/magazine/02self-measurement-t.html?pagewanted=all

Studien über Data Mining, statistische Korrelationen und Prognosen:

Backstrom, Lars; Kleinberg, Jon. 2014. Romantic partnerships and the dispersion of social ties: a network analysis of relationship status on facebook. In Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing (CSCW '14). ACM, New York, NY, USA, 831-841. Online: http://arxiv.org/pdf/1310.6753v1.pdf

Barbaro, M.; Zeller, T.: A Face Is Exposed for AOL Searcher No. 4417749. New York Times, 09.08.2006. Abgerufen am 27.09.2014 von http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all

Bi, Bin; Shokouhi, Milad; Kosinski, Michal; Graepel, Thore (2013): Inferring the Demographics of Search Users, in 22nd International World Wide Web Conference, ACM, 2013: Online: http://research.microsoft.com/pubs/188645/www2013.pdf

Chittaranjan, G.; Blom, J. & Gatica-Perez, D. (2011): Who's Who with Big-Five: Analyzing and Classifying Personality Traits with Smartphones. In: ISWC, IEEE, pp. 29-36. Online: http://infoscience.epfl.ch/record/192371/files/Chittaranjan_ISWC11_2011.pdf

De Bock, K., Van den Poel, D. (2010). Predicting website audience demographics for web advertising targeting using multi-website clickstream data. FUNDAMENTA INFORMATICAE, 98(1), 49–70. http://hdl.handle.net/1854/LU-967442

De Domenico, M.; Lima, A.; Musolesi, M.(2012): Interdependence and Predictability of Human Mobility and Social Interactions. Proceedings of the Nokia Mobile Data Challenge Workshop. Colocated with Pervasive 2012. Newcastle, United Kingdom. June 2012. Online: http://www.cs.bham.ac.uk/research/projects/nsl/mobility-prediction/mdc12.pdf

Eckersley, Peter (2010): How Unique Is Your Web Browser? Electronic Frontier Foundation, 17.05.2010. Online: https://panopticlick.eff.org/browser-uniqueness.pdf

Epp, C.; Lippold, M.; Mandryk, R.L. (2011): Identifying Emotional States Using Keystroke Dynamics. In Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems (CHI 2011), Vancouver, BC, Canada. 715-724. Online: http://hci.usask.ca/uploads/203-p715-epp.pdf

Kosinski, Michal: Stillwell, David; Kohli, Pushmeet; Bachrach, Yoram; Graepel, Thore (2012): Personality and Website Choice, in ACM Web Sciences 2012, ACM Conference on Web Sciences, 2012. Online: http://research.microsoft.com/pubs/163547/person_WebSci_final.pdf

Kosinski, Michal; Stillwell, David; Graepelb, Thore (2013). Private Traits and Attributes Are Predictable from Digital Records of Human Behavior. PNAS, March 2013. Online: http://www.pnas.org/content/110/15/5802

Kramer, Adam D. I.; Guillory, Jamie E. & Hancock, Jeffrey T. (2014): Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences 111 (24), S. 8788–8790. Online: http://www.pnas.org/content/111/24/8788.full

Montjoye, Yves-Alexandre de; Hidalgo, César A.; Verleysen, Michel; Blondel, Vincent D. (2013): Unique in the Crowd: The Privacy Bounds of Human Mobility. Scientific Reports, March 2013, No. 1376. Online: http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html

Montjoye, Yves-Alexandre de; Quoidbach, Jordi; Robic, Florent; Pentland, Alex (2013): Predicting personality using novel mobile phone-based metrics. In: Ariel M. Greenberg, William G. Kennedy, and Nathan D. Bos (Hrsg.): Proceedings of the 6th international conference on Social Computing, Behavioral-Cultural Modeling and Prediction (SBP'13), Springer-Verlag, Berlin, Heidelberg, 48-55. Online: http://web.media.mit.edu/~yva/papers/deMontjoye2013predicting.pdf

Mudholkar, Smita S.; Shende, Pradnya M.; Sarode, Milind V. (2012): Biometrics Authentication Technique for Intrusion Detection Systems Using Fingerprint Recognition. In: International Journal of Computer Science, Engineering and Information Technology, Vol.2, No.1, February 2012. Online: http://airccse.org/journal/ijcseit/papers/2112ijcseit06.pdf

Narayanan, Arvind; Shmatikov, Vitaly (2008): Robust De-anonymization of Large Sparse Datasets. In: Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP '08). IEEE Computer Society, Washington, DC, USA, 111-125. Online: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

Nikiforakis, Nick; Kapravelos, Alexandros; Joosen, Wouter; Kruegel, Christopher; Piessens, Frank; Vigna, Giovanni (2013): Cookieless Monster: Exploring the Ecosystem of Web-based Device Fingerprinting. In: Proceedings of the 34th IEEE Symposium of Security and Privacy (IEEE S&P 2013), San Francisco, CA, USA.

Quercia. D.; Kosinski, M.; Stillwell, D.; Crowcroft, J. (2011): Our Twitter Profiles, Our Selves: Predicting Personality with Twitter. In: Proceedings of SocialCom/PASSAT. 2011, 180-185. Online: https://www.cl.cam.ac.uk/~dq209/publications/quercia11twitter.pdf

Schwartz, H.; Eichstaedt, J.; Kern, M.; Dziurzynski, L.; Ramones, S.; et al. (2013): Personality, Gender, and Age in the Language of Social Media: The Open-Vocabulary Approach. PLoS ONE 8(9): e73791. Online: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3783449/

Sweeney, L. (2002): k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570. Online: http://epic.org/privacy/reidentification/Sweeney_Article.pdf