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.

Kurzfassung

Cracked Labs - Institut für Kritische Digitale Kultur

http://crackedlabs.org

Projektleitung und Autor: Wolfie Christl

Studie im Auftrag der Bundesarbeitskammer

November 2014

Kommerzielle Digitale Überwachung im Alltag: Kurzfassung

„Ihr müsst für eure Privatsphäre kämpfen, oder ihr werdet sie verlieren"
Eric Schmidt, Google (2013)

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.

...intransparente Unternehmen

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.

Ziel der Forschungsarbeit

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 von Verhalten und Verknüpfung persönlicher Daten

Schwangerschaftsprognose aus Einkaufsverhalten

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 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.[1]

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.[2]

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 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.[3]

Praktischer Einsatz von Big Data 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: [4]

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.

---

1 Siehe Kapitel 3.2.2 und 3.2.4
2 Siehe Kapitel 3.2.3 und 3.2.5
3 Siehe Kapitel 3.2.6 und 3.2.7
4 Siehe Kapitel 3.3 und 3.4

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 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.[5]

5 Siehe Kapitel 4.1

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%.[6]

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 Krankenversicherungsprämie. 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.[7]

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 aus-

6 Siehe Kapitel 4.3
7 Siehe Kapitel 4.2

gestatteten 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.[8]

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".[9]

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 intransparent, 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".[10]

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

8 Siehe Kapitel 4.4
9 Siehe Kapitel 5.1
10 Siehe Kapitel 5.2

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.[11]

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.[12]

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.[13]

---

11 Siehe Kapitel 5.3
12 Siehe Kapitel 5.3
13 Siehe Kapitel 5.4

Gesellschaftliche Auswirkungen von kommerzieller digitaler Überwachung[14]

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 wie Kaffee oder jede andere Ware gehandelt werden".

14 Siehe Kapitel 6

Handlungsempfehlungen für Politik, Öffentlichkeit, Unternehmen und BürgerInnen[15]

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**.

15 Siehe Kapitel 6.3.