# BIG DATA IN DER SCHWEIZER SICHERHEITSPOLITIK: EINE ZWISCHENBILANZ EIN JAHR NACH SNOWDEN

*Von Michel Herzog und Tim Prior*

*Die Speicherung, Analyse und Weiterverwendung enormer Datenmengen hat in den letzten Jahren einen technologischen Quantensprung gemacht. «Big Data» verspricht grosse gesellschaftliche Fortschritte, birgt aber auch Missbrauchspotenzial. Die Spannungsfelder zwischen Sicherheit und Freiheit, zwischen Annehmlichkeiten und Datenschutz, zwischen Korrelation und Kausalität sowie zwischen Vertrauen und Verwertbarkeit müssen in politischen Diskussionen und Gesetzesrevisionen neu ausgelotet werden. Im ersten Jahr nach den NSA-Enthüllungen durch Edward Snowden ist in der Schweiz noch kein Umdenken im Umgang mit persönlichen Daten festzustellen. Die Sensibilisierung der Bevölkerung für die Konsequenzen von Big Data, insbesondere für den Schutz der Privatsphäre, steht erst am Anfang.*

## EINLEITUNG

Die Aufdeckung der Operationen des amerikanischen Nachrichtendienstes *National Security Agency* (NSA) und dessen britischen Pendants, der *Government Communication Headquarters* (GCHQ), erregten im Juni 2013 weltweite Aufmerksamkeit. Erstmals wurden die technologischen Möglichkeiten im Bereich der Datensammlung und der Datenanalyse einer breiteren Öffentlichkeit bewusst. Ursprünglich ging der analytischen Datenerhebung die Identifizierung eines Problems voraus, dessen Lösung erforderlich oder zumindest wünschenswert war. Doch im digitalen Zeitalter werden Daten routinemässig über alle Lebensbereiche erhoben, weil deren Speicherung einfach und manchmal auch wichtig ist. Zwar können die gesammelten Daten zu einer Vielzahl nützlicher Zwecke verwendet werden, doch zugleich werden Datenschutz und Schutz der Freiheitsrechte durch den Gebrauch oder aber Missbrauch moderner Technologien zunehmend gefährdet. Auch «Big Data», ein Oberbegriff für die Speicherung und Analyse enormer Datenmengen und deren Weiterverwendung, widerspiegelt diese Ambivalenz: Einerseits verspricht Big Data grosse Fortschritte, andererseits

birgt es ein enormes Missbrauchspotenzial. Eine sachliche, noch zu intensivierende gesellschaftliche Debatte über die positiven und negativen Aspekte bei der Verwendung von neuen technischen Möglichkeiten ist auch in der Schweiz notwendig.

1998 sagte der amerikanische Wirtschaftsprofessor Paul Krugman eine drastische Verlangsamung des Internets voraus. Bis im Jahr 2005, prophezeite er, werde das Internet für die Wirtschaft nicht wichtiger sein als Faxgeräte.[1] Diese grobe Fehleinschätzung verdeutlicht, wie schwer es ist, die Entwicklung von Technologien und deren Verwendung in der Gesellschaft zu antizipieren. Tatsächlich ist heute das Internet in der modernen Informationsgesellschaft das zentrale Medium für den Austausch von Informationen. Die Menge an produzierten und aufgezeichneten Daten ist dramatisch gewachsen. Insbesondere die gewaltige Verbreitung mobiler Endgeräte mit einer Vielfalt eingebauter Sensoren, ein verändertes Kommunikations- und Mitteilungsverhalten mithilfe frei verfügbarer Plattformen wie *Facebook* oder *Youtube,* die Allgegenwärtigkeit der Kommunikationsnetze sowie billiger Speicherplatz und Rechenleistung haben dazu geführt, dass eine kaum vorstellbare Menge verschiedener Daten erzeugt, ausgetauscht und gespeichert werden.

In der Folge gewann ein neuer Begriff in der Fachwelt an Bedeutung: «Big Data». Die Konsequenzen und Möglichkeiten von Big Data wurden von der breiten Öffentlichkeit vorerst nicht zur Kenntnis genommen. Trotz einer Vielzahl warnender Hinweise über potenziell missbräuchliche Anwendungszwecke solcher Datenberge durch staatliche Organe, private Unternehmen und kriminelle Hackerorganisationen wurde der Thematik ausserhalb von Fachkreisen zunächst wenig Beachtung geschenkt.

Big Data ist auch in zunehmendem Mass mit dem Thema Sicherheit sowie nationaler und internationaler Sicherheitspolitik verknüpft, was durch die grossangelegten Datensammlungen und Datenanalysen nationaler Geheimdienste bekräftigt wird. Als zukunftsweisende Technologie wird Big Data bereits in einer Vielzahl von sicherheitsbezogenen Anwendungen eingesetzt oder dies ist in Planung. Nicht medizinische, industrielle oder wirtschaftliche Anwendungen und Herausforderun-

1 Paul Krugman, «Why most economists' predictions are wrong», in: *Red Herring Magazine,* Nr. 55 (1998).

gen werden thematisiert, sondern sicherheitsbezogene staatliche Anwendungsbereiche, welche primär im Kontext der breiten Sicherheitsdebatte stehen. Die sicherheitspolitische Relevanz wird auch durch die ETH-Studie «Sicherheit 2014» unterstrichen, in welcher neu die Datensicherheit als der am stärksten bedrohte Sicherheitsaspekt beurteilt wird. Korrespondierend dazu wird die Wahrscheinlichkeit eines Cyber-Angriffs durch die Bevölkerung am höchsten eingestuft. 34 Prozent des Schweizer Volkes sehen einen Cyber-Angriff als eine wahrscheinliche Bedrohung. Dieser hohe Wert lässt die Vermutung zu, dass es sich dabei um eine direkte Folge der Berichterstattung zum NSA-Abhörskandal handelt.[2] Diese Ergebnisse lassen sich wie folgt interpretieren: Trotz eines generell hohen Sicherheitsempfindens wird eine Ausdehnung der polizeilichen und nachrichtendienstlichen Mittel zur Überwachung mit der Wahrung und/oder dem Ausbau der inneren Sicherheit gerechtfertigt. Es wird aber auch offensichtlich, dass das Thema der Sicherheit von Daten und «Cyber-Security» aktuell ist. Dies darf jedoch nicht als indirektes Einverständnis zu einem Ausbau der Überwachungskapazitäten verstanden werden. Denn gemäss einer noch sich im Gange befindenden internationalen Studie besteht auch in der Schweiz die Sorge einer Aushöhlung der Privatsphäre durch den Einsatz von Überwachungstechnologien.[3] Argumente seitens der Regierung, mit solchen erweiterten Überwachungsmöglichkeiten die Sicherheit und den Schutz der Schweiz zu erhöhen, könnten kritisch hinterfragt werden, wobei insbesondere die zunehmend schwierigere Gewährleistung des Datenschutzes im Kontext der beeindruckenden technischen Entwicklung im Zentrum der Diskussionen stehen dürfte.[4]

**34 Prozent des Schweizer Volkes sehen einen Cyber-Angriff als eine wahrscheinliche Bedrohung.**

2 Tibor Szvircsev Tresch / Andreas Wenger (Hrsg.), *Sicherheit 2014: Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend* (Zürich: ETH Zürich, 2014), 90–96.

3 In der Deutschschweiz befürchten 80 Prozent einen negativen Einfluss, in der Romandie und dem Tessin sind es 77 respektive 69 Prozent. Diese Ergebnisse stehen einem hohen Sicherheitsempfinden in der Schweiz entgegen: Projekt «SurPRISE – Surveillance, *Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe»,* https://www.ta-swiss.ch/projekte/internationale-projekte/surprise.

4 Hanspeter Thür, «Auch du bist verdächtig!», in: *Schweizer Monat,* Nr. 1011 (2013).

Der Sommer 2013 erscheint im Rückblick als Zäsur: Durch die «Snowden-Affäre» rückte insbesondere in Deutschland das Wissen über die gigantische Datensammlung der Geheimdienste NSA und GCHQ die enormen Möglichkeiten der Datenspeicherung und Auswertung ins mediale Rampenlicht. IT-Spezialist Edward Snowden war Ende Mai 2013 mit hochsensiblen NSA-Daten von Hawaii nach Hongkong geflohen und machte die Spähaktionen der NSA am 6. Juni 2013 über den *Guardian* und die *Washington Post* publik.[5] In der Folge wurde der Diskurs in den Themenbereichen «Schutz der Privatsphäre» sowie «Daten- und Persönlichkeitsschutz» – beide ohnehin oftmals durch emotional geführte Debatten geprägt – durch medial verbreitete Schreckensszenarien weiter angeheizt.

**Big Data ist eine Technologie, deren Missbrauch für den Schutz der Privatsphäre gravierende Konsequenzen haben kann.**

Anders als in anderen europäischen Staaten war in der Schweiz jedoch zunächst eine erstaunlich zurückhaltende Atmosphäre der Akzeptanz, ja Indifferenz, zu konstatieren.[6] Im Zusammenhang mit verschiedenen anstehenden Gesetzesrevisionen wäre aber gerade jetzt eine kritische Grundsatzdebatte auch hierzulande notwendig, die nicht im Fahrwasser von aktuellen, medial ins Rampenlicht gerückten Ereignissen stattfindet.

Dieser Beitrag thematisiert die Herausforderungen für die Schweiz im Umgang mit Big Data und den damit verbundenen Möglichkeiten. Ausgangspunkt ist die Überlegung, dass eine kritische Auseinandersetzung mit den Auswirkungen und der Verwendung neuer technologischer Fähigkeiten im Bereich der Datensammlung und -verarbeitung unabdingbar ist.[7] Nur so können künftige Auswirkungen abgeschätzt und unerwünschte Konsequenzen vermieden werden. Big Data ist eine Technologie, die ein grosses Potenzial bietet, deren Missbrauch aber

5 «Nach den NSA-Enthüllungen: Unser Jahr mit Edward Snowden», in: *Frankfurter Allgemeine Zeitung (FAZ)* (07.06.2014); «Ein Erdbeben namens ‹Prism›», in: *FAZ* (06.06.2014).

6 Thür, «Auch du bist verdächtig!».

7 Anthony M. Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia* (New York: Norton & Company, 2005), 14.

vor allem für den Schutz der individuellen Sphäre gravierende Konsequenzen haben kann.

Im Folgenden wird *erstens* das Konzept von Big Data einschliesslich wichtiger Anwendungsmöglichkeiten vorgestellt. Im *zweiten* Abschnitt werden zentrale Problemfelder umrissen, welche sich durch die Verwendung von Big Data ergeben. Dazu werden vier wesentliche Spannungsfelder aufgezeigt. Im *dritten* Kapitel werden Schweizer Gesetzesrevisionen analysiert, die sachlich eng mit der Datenthematik verbunden und derzeit in Bearbeitung sind. Die durch diese Revisionsvorhaben tangierten Problemfelder werden anhand konkreter Beispiele veranschaulicht, ehe im letzten Abschnitt ein Fazit gezogen wird. Das Ziel ist es, eine nüchterne, aber kritische Debatte über die Auswirkungen und Konsequenzen der modernen Informationsgesellschaft anzustossen, in welcher Daten eine immer zentralere Rolle spielen, zugleich jedoch die Gewährleistung des Datenschutzes und der Informationssicherheit eine immer komplexere Aufgabe sein wird.

## 1. BIG DATA UND DESSEN ANWENDUNGSMÖGLICHKEITEN

Big Data polarisiert. Für viele Experten aus dem Technologiesektor stellt die Verwendung von Big Data eine technologische Revolution dar, welche das Leben, Arbeiten und Denken nachhaltig beeinflussen und verändern wird.[8] Sie werden nicht müde, die nahezu grenzenlosen Möglichkeiten hervorzuheben: Verbesserung der Effizienz in Unternehmen und Verwaltungen, Innovation in der Produktion, zielgerichtetes Marketing und effektiveres Management sowie verbessertes Risikomanagement durch genauere Prognosen wie beispielsweise von Naturgefahren. Sicherheitsexperten und Datenschützer heben demgegenüber negative Aspekte hervor, die durch einen Mangel an rechtlichen Schranken bei der Speicherung und Weiterverwendung der Daten und der unüberlegten Anwendung von Algorithmen entstehen.

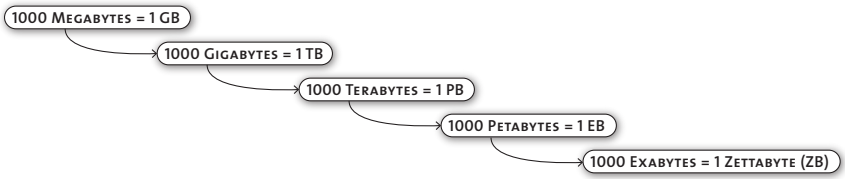
8 Siehe Viktor Mayer-Schönberger / Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think,* 1. Auflage (New York: HMH Publishing, 2013).

## 1.1 WAS IST «BIG DATA»?

Der Begriff «Big Data» kam zum ersten Mal im Jahr 2001 auf und findet seither zunehmende Akzeptanz.[9] Wir leben heute in einem Zeitalter, in dem jeden Tag millionenfach Informationen über verschiedene digitale Kanäle übermittelt werden: Pro Minute werden heute 204 Millionen Emails verschickt, Google erhält über 2 Millionen Suchanfragen, es werden über 100 000 Tweets verschickt und bei Apple werden rund 47 000 Apps heruntergeladen.[10] Folglich wächst die Menge der gespeicherten Informationen in nie dagewesenem Ausmass. Der Datenbestand verdoppelt sich zurzeit alle zwei Jahre. Bis zum Jahre 2020 erwartet die «International Data Corporation» (IDC)[11] einen Datenbestand von 40 Exabytes weltweit, was 40 Trillionen Gigabytes entspricht (siehe Grafik).[12] Aber nicht nur die Gesamtmenge der gespeicherten Informationen wächst in einem rasanten Tempo, auch die Rechenleistung von Computern wird stetig verbessert. Während im Jahr 2003 zur erstmaligen Entschlüsselung eines menschlichen Erbgutes (um die 3 Milliarden Basenpaare) 13 Jahre benötigt wurden, kann eine moderne Forschungseinrichtung die gleiche Menge innert eines Tages sequenzieren.[13]

Das kontinuierliche Wachstum der Informationstechnologie und das Aufkommen des Internets führten zur heutigen Wissens- respektive Informationsgesellschaft, welche überhaupt erst die Rahmenbedingungen

**Von Megabytes bis Zettabytes**




9 Siehe Doug Laney, 3D Data Management: *Controlling Data Volume, Velocity, and Variety* (Stanford: META Group, 2001), 1ff.

10 Omer Tene / Jules Polonetsky, «Privacy in the Age of Big Data – A Time for Big Decisions», in: *Stanford Law Review* 63 (2012).

11 http://www.idc.com/home.jsp.

12 «Datenvolumen verdoppelt sich alle zwei Jahre», in: *Die Welt* (16.07.2013).

13 «DNA Sequencing Is Now Improving Faster Than Moore's Law!», in: *Forbes* (12.01.2012).

für die zunehmend rasante Datengenerierung schafft. Big Data als komplexes Themengebiet hängt in vielfältiger Weise mit dieser Entwicklung zusammen: *Erstens* wird heute jeden Tag eine unüberschaubare Menge an strukturierten, aber vor allem auch unstrukturierten Daten generiert und gespeichert. *Zweitens* nimmt die Bedeutung von mobilen Informations- und Kommunikationstechnologien und Endgeräten stetig zu. *Drittens* haben technische Entwicklungen zu fortgeschrittenen Analysemethoden geführt und so zunehmend komplexe, ressourcenintensive Algorithmen ermöglicht. Der Preis für Speicherkapazität hat sich massiv reduziert und die Rechenleistung moderner Computer konnte deutlich gesteigert werden («Moreschee-Gesetz»). Erst das Zusammenspiel dieser drei Aspekte hat die heutige Datenflut überhaupt ermöglicht – von der Generierung über die Speicherung bis hin zur Auswertung.

Trotz der Aktualität von Big Data unterlassen viele Diskussionsbeiträge eine präzise Definition. Unbestritten scheint, dass das Konzept nicht ausschliesslich auf die enorme Menge an Daten reduziert werden darf. Vielmehr umfasst Big Data verschiedene weitere Aspekte: *Erstens* die technischen Attribute der Daten, *zweitens* die analytischen Fähigkeiten zur Informationsgewinnung und *drittens* die oft vergessenenen technologischen und gesellschaftlichen Entwicklungen, welche die Daten überhaupt erst generieren. Zum besseren Verständnis der Analyse sollen im Folgenden diese drei Aspekte klar definiert werden.

## 1.2 TECHNISCHE ATTRIBUTE

Im Jahr 2001 verwendete der Analyst Doug Laney erstmals die «3 Vs» («Volume», «Velocity», «Variety») als definierende Eigenschaften von Big Data[14]: Das Volumen an Daten, die Geschwindigkeit ihrer Entstehung sowie ihre Verbreitung und Vielfalt (siehe Tabelle auf S. 92). Edd Dumbill definiert «Big Data» als (eine Anzahl von) Daten, welche die Verarbeitungskapazität von herkömmlichen Datenbanksystemen übersteigen. Seiner Ansicht nach sind diese Daten zu gross, bewegen sich zu schnell und/oder passen nicht in die Strukturen von herkömmlichen Datenbank-Architekturen.[15] Offensichtlich ist Big Data damit ein Bereich,

14 Laney, *3D Data Management*.

15 Edd Dumbill, «Making Sense of Big Data», in: *Big Data* 1, Nr. 1 (2013).

**Technische Eigenschaften von Big Data**

**«Volume»:** Das Volumen bezieht sich auf die Menge der Daten (welche mindestens einige Terrabytes beträgt) und die notwendigen Kapazitäten der Datensätze.

**«Velocity»:** Diese Bezeichnung steht für die Geschwindigkeit, mit welcher Daten generiert und gesammelt werden. Um die steigende Menge an Daten zu speichern und analysieren, braucht es immer grössere Speicherkapazitäten und Analysetechnologien.

**«Variety»:** Big Data beinhaltet sowohl strukturierte als auch unstrukturierte Daten aus unterschiedlichen Quellen. Die Herausforderung ist, die Datenformen zusammenzuführen sowie brauchbar und interpretierbar auszuwerten.

welcher hauptsächlich durch seine grösste Herausforderung definiert wird – dem Volumen an unstrukturierten Daten. Insofern überrascht der Fokus auf die Datenmenge nicht.[16] Die Herausforderung bei Big Data ist jedoch, nutzbare Informationen aus denjenigen Daten zu gewinnen, für die analytische Kapazitäten und Ressourcen notwendig sind.

## 1.3 ANALYTISCHE KAPAZITÄTEN

Sowohl eine Vielzahl der analytischen Methoden als auch die für Big Data eingesetzte Software haben ihren Ursprung in Anwendungen der computergestützten Biologie, Medizin und Elektronik, wo sie für die Auswertung grosser Datensätzen entwickelt wurden. Leistungsfähige Algorithmen zum Aufspüren von Mustern, Trends und Korrelationen über verschiedene Zeithorizonte und Datensätze mit unterschiedlichen Datenstrukturen hinweg sind Bestandteil von Big Data. Typischerweise werden auch fortschrittliche Visualisierungstechniken eingesetzt, die Analytikern dabei helfen, die Ergebnisse sinnvoll zu präsentieren und zu verwenden. Die Erkennung von Mustern und Anomalien soll Prognosen ermöglichen, die bei der Entscheidungsfindung helfen sollen. Aus diesem Grund haben Experten das 3V-Modell erweitert, um Faktoren wie Wahrhaftigkeit («veracity»), Wert («value») oder Volatilität («volatility») (siehe Tabelle auf S. 93) einzubeziehen. Verglichen mit den technischen Attributen zielen diese Faktoren darauf ab, die Daten tatsächlich nutzbar zu machen und damit einen Mehrwert zu generieren.

16 Robert Eastman, «Big Data, and Volume, Velocity, and Variety», in: *SMB Research* (2012).

**Analytische Eigenschaften von Big Data**

**«Value»:** Dieser Wert bezieht sich auf den Nutzen, welchen der Anwender durch die Analyse von Big Data erzielt. Dieser Aspekt ist äusserst wichtig, ist er doch der Hauptfaktor für das zunehmende Interesse von Organisationen und Unternehmen an Big Data. Der Erkenntniswert aus den Daten ist dabei nicht nur im monetären Sinn zu verstehen, sondern auch im Sinne besserer Informationen (beispielsweise schnellere und genauere Erkenntnisse).

**«Veracity»:** Dieser Begriff bezieht sich auf die Vertrauenswürdigkeit der Daten, welche in die Analyse einfliessen. Obwohl die hohen Anforderungen an die Standards der Analysen kleinerer Datensätze hinsichtlich Qualität und Vollständigkeit von Big Data nicht vollumfänglich erfüllt werden müssen, ist die Datenqualität von hoher Relevanz, um aussagekräftige und korrekte Analyseergebnisse zu erhalten.

**«Validity»:** Die Frage nach der Validität der Daten ist auch bei der Verwendung von Big Data keinesfalls unwichtig. Offensichtlich gelangt man zu falschen oder unsinnigen Ergebnissen, wenn die verwendeten Daten keinen Beitrag leisten können, um die Analysefrage zu beantworten.

**«Viability»:** Die Brauchbarkeit berücksichtigt, inwieweit die Datenanalyse für spätere Entscheidungen verwendet werden kann.

**«Volatility»:** Die Volatilität sagt aus, wie lange die Daten von Bedeutung sind und beeinflusst somit die Frage, über welche Zeitspanne hinweg sie sinnvollerweise gespeichert werden sollten. Einerseits sinkt durch die Geschwindigkeit der Datengenerierung die Aktualität der bereits gespeicherten Daten rapide, andererseits kann der Einbezug älterer Daten deutlich zuverlässigere Analyseergebnisse hervorbringen.

## 1.4 GESELLSCHAFTLICHE ENTWICKLUNGEN

Die gesellschaftliche Verwendung der technologischen Möglichkeiten ist die treibende Kraft hinter Big Data. Dass wir heute überhaupt über Big Data sprechen, ist ein Nebenprodukt der sogenannten Informationsgesellschaft. Insbesondere mobile Anwendungsgeräte wie Smartphones oder Tablets hinterlassen digitale Datenspuren, die auf vielfältige Weise interpretiert werden können. Die hohe Dichte der Nutzung einer wachsenden Zahl neuer Endgeräte setzt die breite gesellschaftliche Akzeptanz eines entsprechenden Lebensstils voraus. Dazu gehören sowohl ein generell verändertes Kommunikationsverhalten (E-Mail und SMS statt Postbrief) als auch ein verändertes Kaufverhalten (etwa das Online-Einkaufen und Zahlen mit Kreditkarte). In der Schweiz, aber auch in den umliegenden Ländern, nimmt der Anteil des Online-Ver-

sandhandels stetig zu.[17] Die Kommunikation erfolgt via E-Mail, sozialen Medien wie *Facebook* und *Twitter* sowie über Apps wie *WhatsApp*. Weltweit über 500 Millionen Menschen nutzen täglich *WhatsApp* und versenden damit 700 Millionen Bilder pro Tag.[18] Doch die oftmals bequeme Nutzung solcher Dienste kommt nicht ohne ihren Preis. *Erstens* bedeutet ihre Verwendung die Preisgabe einer beträchtlichen Menge an persönlichen Informationen. *Zweitens* ist die Benutzung dieser Dienste kostenlos, weshalb andere Einnahmequellen generiert werden müssen, in deren Zentrum die Daten der Benutzer stehen. Ein anderes Beispiel ist die Verwendung von *Cloud*-Speichern, bei welchen Daten auf einem, dem Benutzer unbekannten, externen Server abgespeichert werden. Auch in diesem Bereich scheinen, gemessen am Wachstums (aktuell sind über 1 Exabyte an Daten in Cloudservices gespeichert), Benutzerfreundlichkeit und Bequemlichkeit vielen Anwendern wichtiger zu sein als offene Fragen bezüglich des Schutzes ihrer Privatsphäre.[19]

## 1.5 ANWENDUNGEN VON BIG DATA

Wie so häufig bei neuen technologischen Möglichkeiten ist deren Verwendung mit Risiken und Problemen behaftet. Experten wie Viktor Mayer-Schönberger und Kenneth Cukier glauben, dass Big Data das Leben, Arbeiten und Denken der heutigen Gesellschaft grundlegend verändern wird.[20] Die Anwendungsbereiche sind sowohl für Unternehmen als auch für Verwaltungen enorm breit.[21] Klimaforscher integrieren Millionen von Beobachtungen täglich und können mithilfe dieser Datensätze Klimawandel-Simulationen durchführen, um so zu besseren Prognosen zu gelangen. Unternehmen wie *Amazon* und *Google* besitzen einen riesigen Fundus an Daten über das Verbraucherverhalten

17 *Online- und Versandhandel Schweiz wächst 2013 mit 9.7%,* 28.02.2014, http://www.gfk.com/ch/news-und-events/presse/pressemitteilungen/Seiten/Online--und-Versandhandel-Schweiz-w%C3%A4chst-2013.aspx.

18 «Rasantes Wachstum: WhatsApp knackt halbe Milliarde», in: *Fokus Online* (23.04.2014).

19 John Callaham, *Research firm: Over 1 exabyte of data is now stored in the cloud,* 20.02.2013, http://www.neowin.net/news/research-firm-over-1-exabyte-of-data-is-now-stored-in-the-cloud.

20 Siehe Mayer-Schönberger/Cukier, «Big Data».

21 *Jaspersoft: Big Data-Projekte nehmen weiter Fahrt auf,* 05.02.2014, http://www.datendschungel.de/2014/markt/jaspersoft-big-data-projekte-nehmen-weiter-fahrt-auf.

und nutzen diese Informationen, um Werbung und Kaufempfehlungen zu personalisieren.[22] Jeder Benutzer des Onlinehändlers und des Suchdienstes kennt die Anzeige zu Produkten, welche kürzlich angeschaut wurden oder einen thematischen Bezug zu bereits bestellten Produkten aufweisen. Ein anderes Beispiel ist die Kriminalprävention. Polizeidienste speichern grosse Datensätze über frühere Verbrechen, mit deren Hilfe Muster und Verhalten analysiert werden und damit präventive Verbrechensabwehr betrieben wird.[23] Auch die Stadtpolizei Zürich hat, als erste Polizei einer Grossstadt in Europa, mit der Prognosesoftware «PRECOGS» bereits ein System im Testbetrieb, mit dessen Hilfe die Verbrechensbekämpfung effizienter und effektiver gestaltet werden soll.[24]

Dies sind nur einige wenige Beispiele, bei welchen Big Data schon heute angewendet wird. Auch die Vielzahl möglicher Online-Kommunikationsmittel ist ein wichtiger Lieferant von Daten, deren Analyse für Behörden und Unternehmen einen Mehrwert bringen kann.[25] «Twittern», das Surfen im Internet und Herunterladen von Inhalten, der Kauf von Gütern, der Austausch von Nachrichten via E-Mail oder *Instant Messaging* kombiniert mit der allgegenwärtigen Geo-Referenzierung eröffnen grosse Möglichkeiten. Die Kehrseite der Medaille ist jedoch auch eine zunehmend lückenloses Überwachungspotenzial der einzelnen Benutzer. Mit zunehmenden Fortschritten in der Soft-und Hardware, den grossen Datenmengen (Big Data) und der Aggregation der Daten wird ein ständig wachsender Einblick in das Leben des Einzelnen möglich.

## 2. SPANNUNGSFELDER

Big Data stellt neue Herausforderungen für den Datenschutz und den Schutz der Privatsphäre dar. Zwar sind laut einer Studie die meisten Big-Data-Projekte in den USA im Bereich Wissenschaft, Weltraum und Technologie angesiedelt, auf zweitem Rang kommen jedoch bereits Pro-

22 *Privacy-Handbuch,* https://www.privacy-handbuch.de/handbuch_12.htm.

23 *Memphis Police Department Reduces Crime Rates with IBM Predictive Analytics Software,* 21.07.2010, http://www-03.ibm.com/press/us/en/pressrelease/32169.wss.

24 http://www.inside-it.ch/articles/37852; http://www.ifmpt.de/aktuelle-presserklarung-vom-22-04-2014.

25 «Blossgelegte Freundschaften», in: *Tages-Anzeiger* (07.08.2013).

jekte im Bereich der nationalen Verteidigung, der Nachrichtendienste und der Cyber-Security, gefolgt von «Homeland Security» und der Kriminalitätsbekämpfung auf dem dritten Rang.[26] Diese Entwicklung wird kaum rückgängig zu machen sein. Sie birgt verschiedene Spannungsfelder, welche im Folgenden veranschaulicht werden und auch in der Schweiz als Diskussionsgrundlage für gesellschaftliche, politische und rechtliche Debatten verstanden werden sollen.

## 2.1 SICHERHEIT VS. FREIHEIT

Die Werte «Sicherheit» und «Freiheit» stehen in einem Wechselverhältnis zueinander. Um in Freiheit zu leben, braucht es Sicherheit. Doch die Bemühungen um Sicherheit können auch Freiheiten einschränken. Sowohl Freiheit als auch Sicherheit sind in westlichen Gesellschaften wichtige Werte und deshalb in besonderem Mass schützenswert.[27] Doch um wessen Sicherheit und um welche Art von Sicherheit geht es? Sicherheit ist die Abwesenheit von Schaden. Dieser kann von der Natur ausgehen, wie bei Erdbeben, oder von Menschen gemacht sein, wie im Falle von Kriegen. Schaden ist eine Einschränkung von Freiheit. Unbestritten ist, dass es zu den Aufgaben des Staates gehört, für die Sicherheit seiner Bürger zu sorgen, wodurch die Freiheit des Einzelnen gewährleistet wird.[28] Doch wie weit darf ein Staat gehen, um die Allgemeinheit vor Gefahren zu schützen? Wie weitgehend dürfen moderne Überwachungstechnologien und Analysemethoden eingesetzt werden?

Dieses Spannungsverhältnis wird durch den technologischen Fortschritt weiter verschärft. Geht es um die Verwendung neuer Technologien, wird oftmals mit dem Argument der Sicherheit argumentiert. Durch ein vermeintlich vorteilhaftes Kosten-Nutzen-Verhältnis verspricht man sich eine starke Erhöhung der Sicherheit. Auch im Diskurs

26 Alex Rossino, *Estimating Federal Big Data Spending,* 01.10.2013, https://iq.govwin.com/index.cfm?fractal=blogTool.dsp.blog&blogname=public&alias=Estimating-Federal-Big-Data-Spending.

27 Sandro Gaycken, *Jenseits von 1984: Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft: Eine Versachlichung* (Bielefeld: Transcript, 2013), 8.

28 Gabriel Brönnimann, «Die umkämpfte Einführung der Vorratsdatenspeicherung in der EU», in: Sandro Gaycken (Hrsg.), *Jenseits von 1984: Datenschutz und Überwachung in der fortgeschrittenen Informationsgesellschaft: Eine Versachlichung* (Bielefeld: Transcript, 2013), 55.

um Big Data finden wir das Sicherheitsargument wieder. Die datengestützte Prognose von Verbrechen *(Predictive Policing)* wird von ihren Befürwortern mit einer Erhöhung der Sicherheit gerechtfertigt. Die Echtzeitanalyse von Überwachungskameras, sozialen Medien und anderen Kommunikationskanälen wird ebenfalls damit begründet.[29] Allerdings geht diese erhöhte Sicherheit zulasten einer ständig zunehmenden Überwachung durch elektronische Systeme. In der heute existierenden Überwachungsära verschiebt Technologie die Macht weiter zu Gunsten des bereits mächtigen Staates und seiner Dienste.[30]

Auch die Schweiz steht vor der Frage, wie die Gewichtung der beiden essenziellen Werte Freiheit und Sicherheit künftig gestaltet werden soll. Beide werden in Art. 2 der Bundesverfassung als Zweck der Schweizerischen Eidgenossenschaft genannt. Ihre gegenseitige Abhängigkeit tritt in Art. 10 BV (Recht auf Leben und auf persönliche Freiheit) besonders klar hervor. Auch einige der laufenden Gesetzesrevisionen (siehe Kapitel 3) bewegen sich genau in diesem Spannungsfeld. Mehr Daten und mehr Überwachung müssen nicht einen sofortigen Verlust von Freiheit bedeuten – was aber nicht bedeutet, dass sie nie einen Verlust von Freiheit hervorrufen werden.[31] Insbesondere die präventiven Kompetenzen, welche im neuen Nachrichtendienstgesetz (NDG) vorgesehen sind, scheinen diesbezüglich problematisch, da mit diesen bereits die gefühlte Freiheit beeinträchtigt wird. Es braucht daher ein Höchstmass an Transparenz und Kontrolle.

**Diese erhöhte Sicherheit geht zulasten einer ständig zunehmenden Überwachung durch elektronische Systeme.**

29 IBM beschreibt dies folgendermassen: «To more effectively predict and prevent threats, government organizations must be capable of managing numerous data types and use advanced, real-time analytics designed to transform data into insights.» http://www-01.ibm.com/software/data/bigdata/industry-government.html.

30 Michael Mimoso, Bruce Schneier: *Technology Magnifies Power in Surveillance Era,* 09.04.2014, https://www.schneier.com/news-180.html.

31 Brönnimann, «Umkämpfte Einführung».

## 2.2 ANNEHMLICHKEIT VS. DATENSCHUTZ

Ohne Zweifel muss das Konzept des Datenschutzes in absehbarer Zukunft angepasst werden. Bestehende Datenschutzgesetze sind mit den modernen Informationstechnologien und der Lebensweise des «digitalen Bürgers» überfordert. Daten werden zur Währung und damit zur wertvollen Ressource.[32] Politik und Justiz gewährleisten lediglich das Selbstbestimmungsrecht über persönliche Daten. Der Entscheid, ob die Annehmlichkeit der modernen Technologie, welche wohl kaum ohne ein Mindestmass an Offenheit zu haben sein wird, oder die eigene Privatsphäre höher gewichtet wird, liegt letztlich beim Einzelnen. Die Signale als Folge der NSA-Affäre sind unterschiedlich: So kommt eine Umfrage zum Schluss, dass vier von fünf Personen in den USA zwischen Juni und November 2013 in den sozialen Medien die Privatsphäreneinstellungen ihrer Nutzerkonten geändert haben.[33] Ferner wird der Datenverkehr im Internet vermehrt verschlüsselt und die Skepsis gegenüber *Cloud*-Speicherlösungen ist gestiegen.[34] Auch der Wunsch nach weniger Abhängigkeit von amerikanischer Soft- und Hardware weist auf eine gestiegene Sensibilität hin.[35] Insgesamt kann davon ausgegangen werden, dass immer mehr Personen, zumindest kurzfristig, eine Sensibilität für die sicherheitsrelevanten Aspekte der Cyber-Thematik und wie Datensicherheit entwickeln.[36] Inwiefern dies einen langfristigen Trend darstellt, lässt sich nicht abschliessend beurteilen. Beim individuellen Umgang mit persönlichen Daten muss letztlich jede Person selbst entscheiden, wieviel Annehmlichkeiten sie sich durch die Verwendung moderner, datenbezogener Technologien

**Vier von fünf Personen in den USA änderten zwischen Juni und November 2013 in den sozialen Medien die Privatsphäreneinstellungen ihre Nutzerkonten.**

32 Michael Mimoso, *Bruce Schneier: Technology Magnifies Power in Surveillance Era,* 09.04.2014, https://www.schneier.com/news-180.html

33 «Snowden-Effekt»: Jugend achtet auf eigene Daten», in: *News.ch* (19.11.2013).

34 «Folgen der NSA-Affäre: Wie Snowden das Netz verändert hat», in: *Spiegel Online* (07.06.2014).

35 «Aigner warnt vor Abhängigkeit von US-Konzernen», in: *Die Welt* (12.07.2013).

36 Szvircsev Tresch / Wenger, *Sicherheit 2014,* 90.

«erkaufen» möchte. Wichtig ist, dass das Bewusstsein gestärkt wird, dass diese Dienstleistungen einen Preis haben, auch wenn dieser nicht mit einem Preisschild daherkommt.

## 2.3 KORRELATION VS. KAUSALITÄT

Einer der wichtigsten Vorteile von Big Data ist die Möglichkeit, Daten nach Mustern zu analysieren. Dadurch können Unternehmen wertvolle Informationen erlangen, um das Konsumverhalten ihrer Kunden zu analysieren, vorherzusagen oder gar zu steuern. Auch in der Politik und bei administrativen Entscheidungsprozessen stellt solches Wissen die Basis für Entscheidungsprozesse dar. Um den Nutzen von Big Data zu bestimmen, sollte jedoch zwischen Korrelation und Kausalität unterschieden werden. Eine Korrelation ist eine wechselseitige Beziehung zwischen zwei oder mehr Faktoren. Wird ein Faktor verändert, so beeinflusst dies auch den anderen. Zum Beispiel besteht eine Korrelation zwischen Bildungsgrad und Gesundheit, welche in der Regel durch die durchschnittliche Lebenserwartung in einer Gesellschaft angegeben wird.[37] Allerdings bedeutet Korrelation nicht Kausalität: Menschen leben nicht deswegen länger, weil sie gebildet sind.

In einer Diskussion über den Nutzen von Big Data in der politischen Praxis und seitens der Behörden ist die Unterscheidung zwischen Korrelation und Kausalität zentral. Wiederholt konnten Prognosen, die auf scheinbaren Kausalitäten beruhten, nicht halten, was sie versprachen. Als prominentestes Beispiel in diesem Zusammenhang wird immer wieder «Flu Trends» von Google genannt.[38] Daher muss eine Debatte darüber geführt werden, ob die Zusammenführung von kausal

37 David M. Cutler / Adriana Lleras-Muney, «Education and Health: Evaluating Theories and Evidence», in: Robert F. Schoeni et al. (Hrsg.) *Making Americans Healthier: Social and Economic Policy as Health Policy* (New York: Russell Sage Foundation, 2008), 10ff.

38 Als prominentestes Beispiel in diesem Zusammenhang wird immer wieder «Flu Trends» von Google genannt. Google «Flu Trends» versucht, basierend auf der Annahme, dass die Häufigkeit bestimmter Suchbegriffe Anhaltspunkte auf eine Grippeerkrankung gibt, Prognosen über anstehende Grippeerkrankungen geben zu können. Diese sollen sich bezüglich der Genauigkeit als auch im Hinblick auf die Vorwarnzeit besser sein als die offiziellen Daten der Behörden. Vgl. David Lazer / Ryan Kennedy / Gary King / Alessandro Vespignani, «The Parable of Google Flu: Traps in Big Data Analysis», in: *Science* Bd. 343 (2014).

nicht zusammenhängenden Daten bei der Lösung von sachlichen Problemen dienlich ist.

Sich über den Unterschied zwischen Korrelation und Kausalität bewusst zu werden, ist für politischen Entscheidungsträger in der Schweiz von grosser Bedeutung. Dies gilt, auch wenn die praktische Verwendung von Big Data durch die Behörden derzeit noch kein Thema ist. Big Data kann ich vielen Bereichen sehr wertvolle Erkenntnisse beisteuern, ersetzt aber nicht eine wohlüberlegte Fragestellung und eine qualitative Auseinandersetzung mit den Ursachen und Gründen eines Problems.

## 2.4 VERTRAUEN VS. VERWERTBARKEIT

Bei der Verwendung von Big Data sind auch moralische Überlegungen relevant: Ist es beispielsweise vertretbar, dass eine (private, öffentliche oder nicht-staatliche) Organisation Daten von Menschen ohne konkreten Grund sammelt und weiterverwendet? Sollen Daten auch auf Vorrat gesammelt werden dürfen, wenn mit ihnen, zumindest zum Zeitpunkt der Generierung und Abspeicherung, keine konkreten Fragen beantwortet oder Probleme gelöst werden können?

**Die Enthüllungen Snowdens erhöhten die Attraktivität der Schweiz als Datenbankanbieter und als Standort für Rechenzentren.**

Die Snowden-Affäre hat gezeigt, in welchem Ausmass US-Regierungsstellen Daten sammeln, speichern und analysieren. Die Nutzung von Big Data wird seither von der Öffentlichkeit kritischer hinterfragt. Wegen der vergleichsweise strikten Datenschutzgesetze in der Schweiz haben die Enthüllungen Snowdens die Attraktivität der Schweiz als Datenbankanbieter und als Standort für Rechenzentren erhöht.[39] Verglichen mit den USA oder dem restlichen Europa finden Kunden in der Schweiz eine sicherere Alternative für *Cloud-Computing*-Leistungen.

Zudem scheint die Schweizer Regierung in Bezug auf Datenschutz und -nutzung als gutes Beispiel voranzugehen. Vertrauen und Transparenz, sowohl seitens der Anbieter als auch der Behörden, sind in diesem

39 Brigitte Strebel, «Die Schweiz, die Cloud und die Sicherheit», in: *Mediaplanet* (September 2013).

Bereich ein kostbares Gut und im internationalen Umfeld derzeit ein komparativer Vorteil. Im April 2014 lancierte die Schweizer Regierung das Pilotportal für offene Behördendaten der Schweiz als Teil der Open-Government-Data-Strategie Schweiz von 2014 bis 2018.[40] Zwar enthält das Portal zum jetzigen Zeitpunkt nicht alle Regierungsinformationen, doch es zielt darauf ab, der Öffentlichkeit Daten bereitzustellen, welche die Transparenz im politischen Prozess erhöhen und die politische Partizipation fördern soll. Damit soll in der Schweiz eine Kultur der offenen Regierungsdaten geschaffen werden. Die Einhaltung der Privatsphäre gilt dabei als Voraussetzung. Dieser offene und transparente Umgang mit Daten ist ein Schritt in die richtige Richtung.

## 3. DATENBEZOGENE DEBATTEN UND REVISIONSVORHABEN IN DER SCHWEIZ

Die NSA-Affäre löste politische Diskussionen aus, die für die Big Data-Debatte ebenfalls relevant sind. Eine Motion des Ständerats Paul Rechsteiner, welche in leicht abgeänderter Form von National- und Ständerat gegen den Willen des Bundesrates angenommen wurde, verlangte die Bildung einer Expertenkommission, welche sich in Hinblick auf technologische und politische Entwicklungen mit der Zukunft der Datenbearbeitung und der Datensicherheit auseinandersetzen soll.[41]

Eine Konsequenz aus der NSA-Affäre zog der Bundesrat anfangs 2014. So sollen zukünftig besonders kritische und zentrale Leistungen im Bereich der Telekom- und Informatikanlagen nur noch bei Schweizer Unternehmen eingekauft werden. Allerdings stehen nicht für alle benötigten Dienstleistungen Schweizer Anbieter zur Verfügung.[42] Ebenfalls wurde der Bundesanwaltschaft die Freigabe erteilt, im Zusammenhang mit der US-Geheimdienstaffäre wegen Spionage in der Schweiz zu ermitteln.[43] Zudem wurden verschiedene Departemente angewie-

40 *Was ist opendata.admin.ch?,* 16.09.2014, http://www.opendata.admin.ch/de/about.

41 Schweizer Parlament, *Motion zur Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit*, 26.09.2013.

42 *NSA-Affäre: Bund schliesst ausländische IT-Anbieter (teilweise) aus,* 05.02.2014, http://www.inside-it.ch/articles/35270.

43 «NSA-Affäre: Bundesrat gibt grünes Licht für Strafverfahren», in: *Neue Zürcher Zeitung (NZZ)* (06.12.2013).

sen, die Sachlage zu klären und allenfalls notwendige Massnahmen vorzuschlagen.[44]

Zurzeit sind in der Schweiz diverse Gesetzesrevisionen in Arbeit, welche einerseits mit dem Datenschutz Berührungspunkte aufweisen, andererseits im Lichte der Snowden-Affäre eine neue Brisanz innehaben. Betroffen sind die Revisionen des Nachrichtengesetzes (NDG), des Bundesgesetzes zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) sowie des Datenschutzgesetzes (DSG). Die beiden ersten Revisionen streben eine Ausweitung der staatlichen Massnahmen und Möglichkeiten zur Überwachung an, mit deren Hilfe die zuständigen Dienste ihre Aufgaben besser wahrnehmen können sollen.

### 3.1 REVISION DES NACHRICHTENDIENSTGESETZES

Mit der Ausarbeitung des neuen Nachrichtendienstgesetzes (NDG) hat der Bundesrat das Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) bereits 2009 beauftragt. Damit sollen das Bundesgesetz über Massnahmen zur Wahrung der Inneren Sicherheit (BWIS) und das Bundesgesetz über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (ZNDG) ersetzt werden. Das Vernehmlassungsverfahren wurde am 30. Juni 2013 abgeschlossen.[45] Ein Entwurf wurde am 19. Februar 2014 publiziert – die parlamentarische Beratung ist im Gange.[46] Ziel ist es, den Nachrichtendienst des Bundes (NDB) auf real existierende Bedrohungen im Cyber-Bereich, auf den Schutz des Wirtschafts- und Finanzplatzes Schweiz sowie gegen Spionage und Terrorismus auszurichten. Nebst organisatorischen Umstrukturierungen sind gemäss Art. 25 des neuen NDG auch neue inhaltliche, bewilligungspflichtige Informationsbeschaffungsmassnahmen vorgesehen:

> *a.* Überwachung des Post- und Fernmeldeverkehrs nach BÜPF; *b.* der Einsatz von Ortungsgeräten zur Feststellung des Standorts und der Bewegung von Personen oder Sachen; *c.* der Einsatz von Überwachungsgeräten […];

44 «Bundesrat reagiert auf NSA-Affäre: VBS prüft Massnahmen», in: *NZZ* (20.09.2013).

45 *Ergebnisbericht zum Vernehmlassungsentwurf zum Nachrichtendienstgesetz (NDG)*, 22.10.2013.

46 *Nachrichtendienstgesetz*, http://www.vbs.admin.ch/internet/vbs/de/home/themen/ndb/uebersicht.html.

> *d.* das Eindringen in Computersysteme und Computernetzwerke zur Informationsbeschaffung oder zur Störung fremder Informationsbeschaffung bei Angriffen auf kritische Infrastrukturen; *e.* das Durchsuchen von Räumlichkeiten […].[47]

Befürworter argumentieren, dass die NSA-Affäre eindrucksvoll die Notwendigkeit eines verbesserten Nachrichtendienstes mit erweiterten Kompetenzen zum Schutz der Schweiz vor aktuellen Bedrohungen und Gefahren demonstriert hat.[48] Betont wird auch, dass damit keine flächendeckende Aufklärung und Überwachung betrieben wird und strenge rechtliche und politische Mechanismen die individuelle Freiheit schützen. Insgesamt wird jährlich mit zehn Fällen von präventiver Überwachung gerechnet, welche bei Terrorismus, Proliferation, Spionage und Gewaltextremismus sowie zur Wahrung wesentlicher Landesinteressen in besonderen Lagen, etwa dem Schutz kritischer Infrastrukturen, erlaubt wären.[49] Jüngste Ereignisse, beispielsweise im Zusammenhang mit aus Syrien in die Schweiz zurückkehrenden einheimischen Dschihadkämpfern, werden seitens der Befürworter als Rechtfertigung der Ausweitung der Überwachungsmöglichkeiten angeführt.[50] Gegner sehen in diesen Revisionsvorhaben hingegen eine starke Ausweitung der Überwachung und zweifeln die Notwendigkeit und Verhältnismässigkeit einiger Aspekte an, darunter auch den Einsatz von Trojanern.[51]

Speziell der Einsatz von Trojanern wird – jenseits rechtlicher Probleme – aus folgenden Gründen oft kritisch betrachtet: *Erstens* stellt

47 Neues Nachrichtendienstgesetz (NDG), Art. 25.

48 Schweizer Parlament, *Die aktuell wichtigsten Geschäfte der Sicherheitspolitischen Kommissionen,* Juni 2014.

49 Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), *Welche neuen «Werkzeuge» erhält der NDB mit dem neuen NDG?,* 16.09.2014.

50 http://www.thomas-hurter.ch/phocadownloadpap/userupload/Publisher/2014-09-18_Mit%20Nachrichtendienstgesetz%20gegen%20IS.pdf.

51 *Dossier: Totalrevision BÜPF,* 18.01.2014, https://www.digitale-gesellschaft.ch/2014/01/18/dossier-totalrevision-buepf. Trojaner sind eine Kategorie von Schadsoftware, welche nebst ihrer eigentlichen Funktion noch weitere, dem Nutzer unbekannte Funktionen haben. Bei ihrer Ausführung werden oftmals Datenbestände und Passwörter ausspioniert und über die bestehende Internetverbindung weiterversendet, aber auch Systemkonfigurationen verändert oder gelöscht. «Trojaner», in: *Das grosse Online-Lexikon für Informationstechnologie* (16.09.2014), http://www.itwissen.info/definition/lexikon/Trojaner-trojan.html.

sich die Frage, wo staatliche Organe die Software beschaffen. *Zweitens* besteht die Gefahr, dass die durch die Schadsoftware entstandenen Sicherheitslücken auch von anderen Parteien ausgenutzt werden. *Drittens* besteht ein beträchtliches Missbrauchspotenzial seitens der Behörden, beispielsweise durch Möglichkeiten der Ausspähung, welche weit über den gesetzlichen Auftrag hinausgehen.[52] Insbesondere die Kritiker sehen sich in ihrer Meinung durch die NSA-Enthüllungen bestätigt und warnen vor den negativen Konsequenzen auf die Freiheitsrechte, welche eine Ausweitung präventiver Überwachungskompetenzen mit sich bringt.[53]

Es scheint deshalb aufgrund zunehmender Kritik am neuen NDG möglich, dass gegen das Gesetz das Referendum ergriffen wird – mitunter sicherlich auch deshalb, weil die Exzesse der US-Geheimdienste generell das Vertrauen in Nachrichtendienste untergraben haben. Zudem gehen die Möglichkeiten der präventiven Überwachung selbst Exponenten des bürgerlichen Lagers (Jungparteien) einen Schritt zu weit.[54]

### 3.2 REVISION DES BUNDESGESETZES ZUR ÜBERWACHUNG DES POST- UND FERNMELDEVERKEHRS

Im Falle der Revision des Bundesgesetzes zur Überwachung des Post- und Fernmeldeverkehrs BÜPF gestaltet sich die Debatte ähnlich, wenn auch die Kritik milder ausfällt, da es um Strafverfolgung geht, womit das Vorhaben keine präventiven Massnahmen beinhaltet und damit auf weniger Skepsis stösst. Im Mai 2010 schickte der Bundesrat die Totalrevision dieses Bundesgesetzes in die Vernehmlassung, welche Ende November 2011 abgeschlossen war. Die Botschaft zum Bundesgesetz und der Entwurf wurden am 27. Februar 2013 veröffentlicht.[55] Als Grund für die Revision führt das EJPD die technischen Entwicklungen an, welche es mutmasslichen Straftätern mithilfe verschlüsselter Kommunikation und dem Internet zunehmend erleichtern, einer Überwachung

52 «CCC enttarnt Staatstrojaner», in: *Zeit Online* (08.10.2011).

53 Daniel Vischer, *Snowden und das neue Nachrichtendienstgesetz,* Juli 2013, http://www.vimentis.ch/d/dialog/readarticle/snowden-und-das-neue-nachrichtendienstgesetz.

54 «Kritik am Nachrichtendienstgesetz wächst: Neues Ungemach für Ueli Maurer», in: *NZZ* (13.06.2014).

55 https://www.bj.admin.ch//bj/de/home/sicherheit/gesetzgebung/fernmeldeueberwachung.html

durch die Strafverfolgungsbehörden zu entgehen. Dabei wird betont, dass es nicht um mehr, sondern um gezieltere Überwachung gehe.[56] Auch wenn die Befürworter betonen, dass es primär um eine klare gesetzliche Grundlage zum Einsatz von Informatikprogrammen seitens der Behörden geht, gibt es auch umstrittenere Aspekte.[57] So kritisieren Gegner, dass die Vorratsdatenspeicherung mit der Revision von 6 auf 12 Monate ausgedehnt wird, der Einsatz von Bundestrojanern und IMSI-Catcher[58] legalisiert und der Geltungsbereich, wie etwa auf WLANs in Wohngemeinschaften, unverhältnismässig ausgedehnt wird.[59] In der Konsequenz steht die Lancierung eines Referendums von verschieden Seiten zur Debatte.[60]

### VORRATSDATENSPEICHERUNG IM INTERNATIONALEN VERGLEICH

Im Vergleich zu den umliegenden europäischen Staaten sieht die Schweizer Gesetzgebung weitgehende Befugnisse im Bereich der Speicherung von Daten vor. So müssen in der Schweiz die Telekomanbieter das Kommunikationsverhalten ihrer Kunden aufzeichnen (sogenannte Meta-Daten, darunter die Gesprächsdauer, wann, wie lange und wo ins Internet eingeloggt wurde, wem eine E-Mail oder SMS gesendet wurde sowie die Standortinformationen des Mobilgerätes). Diese «rückwirkende Überwachung» ist im Gesetz vorgesehen und verpflichtet die Anbieter gemäss Art. 15. BÜPF, die Daten für sechs Monate zu speichern. Auf Verlangen erhalten die Strafverfolgungsbehörden im Rahmen einer Untersuchung Zugang zu diesen Informationen. Im Rahmen der Revision des BÜPF soll diese Frist auf 12 Monate verdoppelt werden. Eine Beschwerde der Digitalen Gesellschaft Schweiz gegen die generelle Vorratsdatenspeicherung wurde vom Bund zurückgewiesen.[61]

Auch international gerät die Vorratsdatenspeicherung zunehmend unter Druck. Eine Richtlinie der EU zur Vorratsdatenspeicherung, die eine Speicherdauer zwischen 6 und 24 Monaten vorsah, war zwischen 2006 und 2014 in Kraft, ehe sie vom europäischen

56 Ebd.

57 Eidgenössisches Justiz- und Polizeidepartement (EJPD), *Überwachung des Fernmeldeverkehrs: Zeitgemässe und klare Rechtsgrundlage*, 27.02.2013.

58 Die «International Mobile Subscriber Identity» (IMSI) ist eine Benutzernummer, welche auf der Mobilfunkkarte jedes Mobiltelefons gespeichert ist. Mit einem solchen Empfängergerät («Catcher») kann diese Nummer ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt sowie die laufenden Telefonate eines Mobiltelefons abgehört werden.

59 *Breit abgestütztes Referendum gegen BÜPF-Revision*, 27.05.2014, https://www.digitale-gesellschaft.ch/2014/05/27/breit-abgestuetztes-referendum-gegen-buepf-revision/#more-3280.

60 Ebd.

61 «Bund weist Beschwerde gegen Vorratsdatenspeicherung ab», in: *NZZ* (01.07.2014).

Gerichtshof am 8. April 2014 für unzulässig erklärt wurde. Das Gericht beurteilte die Vorratsdatenspeicherung als «Eingriff von grossem Ausmass und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, der sich nicht auf das absolut Notwendige beschränkt». Zudem werde durch die Speicherung der Telefon- und Internetdaten und des Zugriffes darauf ohne das Wissen der Betroffenen ein Gefühl der ständigen Überwachung des Privatlebens hervorgerufen.[62] In Deutschland wurde die Umsetzung der umstrittenen EU-Richtlinie schon im Jahre 2010 durch das Bundesverfassungsgericht verhindert.[63]

Die politischen Reaktionen innerhalb der EU auf den Entscheid des EuGH fanden erstaunlicherweise bisher kaum Beachtung in der Schweizer Debatte. Rechtlich ist er ohnehin nicht bindend für die Schweiz als Nichtmitglied der EU. Die Befürworter betonen weiterhin, dass ein öffentliches Interesse an der Aufklärung von schweren Straftaten besteht, das diese Massnahme rechtfertigt.[64] Es bleibt abzuwarten, ob die veränderte internationale Sachlage einem allfälligen Referendum Aufwind verleiht.

## 3.3 DER DATENSCHUTZ IN DER SCHWEIZ UND BIG DATA

Während es bei den beiden obengenannten Gesetzesrevisionen hauptsächlich um die Mittel und Kompetenzen bei der Informationsbeschaffung geht, kann Big Data ebenso für den Datenschutz eine riesige Herausforderung darstellen und die Privatsphäre bedrohen. Bei eingehender Betrachtung der Terminologie des aktuellen Datenschutzgesetzes und der wesentlichen Elemente von Big Data treten erhebliche Diskrepanzen zutage.[65] *Erstens* sieht Art. 4 Abs. 4 DSG vor, dass die Datenbeschaffung und der Bearbeitungszweck erkennbar sein müssen; Big Data geht grundsätzlich von einer unbeschränkten Zahl von Datenquellen, Bearbeitungszwecken und Datenempfängern aus sowie einem oftmals unbekannten Speicherort. Die Transparenz ist somit keinesfalls sichergestellt. *Zweitens* besagt Art 4. Abs. 3 DSG, dass der Bearbeitungszweck bei der Beschaffung ersichtlich oder gesetzlich vorgeschrieben sein muss. Big Data hingegen ist gekennzeichnet von einer dynamischen Zweckbestimmung, keiner gesetzlichen Bearbeitungspflicht und eben auch durch die Analyse von verschiedensten Daten ausserhalb des

62 «Gegen die Vorratsdatenspeicherung: Europäischer Gerichtshof kippt Überwachung», in: *Netzwoche* (08.04.2014).

63 «Karlsruhe stoppt Vorratsdatenspeicherung: Merkel warnt vor einem Vakuum», in: *FAZ* (02.03.2010).

64 «Bund rechtfertigt Vorratsdatenspeicherung», in: *NZZ* (01.07.2014).

65 Vgl. *Erläuterungen zu Big Data,* http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=de.

Beschaffungskontextes. Die Zweckbindung scheint insofern nicht erfüllt. *Drittens* besagt Art. 4 Abs. 2 DSG, dass die Bearbeitung geeignet, erforderlich und verhältnismässig sein muss. Dies steht in diametralem Widerspruch zum Wesenskern von Big Data, welches nach maximalen Datenbeständen strebt, da Masse über den Analyseerfolg entscheidet und Datensparsamkeit somit unerwünscht ist. Die Verhältnismässigkeit muss somit ebenfalls angezweifelt werden. *Viertens* verlangt Art. 4 Abs. 5 DSG, dass bei der Bearbeitung von Personendaten die Einwilligung der betroffenen Personen erforderlich ist und dass diese Einwilligung erst nach angemessener Information wissentlich und somit freiwillig erfolgt. Bei besonders schützenswerten Personendaten muss die Einwilligung zudem ausdrücklich erfolgen. Inwiefern diese Vorgehensweise bei der Verwendung von Big Data realisierbar ist, bleibt offen. Zudem ist der Umfang der Bearbeitung unklar, die Bearbeitungsparameter sind dynamisch, und der Nutzer sehr wahrscheinlich überfordert. Eine Einwilligung einzuholen, scheint deshalb schwierig zu sein. Inwiefern die Anonymisierung der Daten dies zu entkräften vermag, bleibt fraglich, da diverse Beispiele zeigen, dass anonymisierte Daten oder Meta-Daten durchaus Rückschlüsse auf die Person und ihre Präferenzen zulassen.[66]

**Anonymisierte Daten oder Meta-Daten lassen durchaus Rückschlüsse auf die Person und ihre Präferenzen zu.**

Die zunehmende Benutzung von Big Data ist ein Fakt. Dass somit eine grundlegende Überprüfung und allfällige Überarbeitung des Datenschutzgesetzes notwendig ist, wurde seitens der Behörden erkannt.[67] Basierend auf einer Evaluation des Datenschutzgesetzes beauftragte der Bundesrat am 9. Dezember 2011 das EJPD, gesetzgeberische Massnahmen zur Stärkung des Datenschutzes zu prüfen. Bis Ende 2014 sollen dem Bundesrat durch eine Expertengruppe erarbeitete Massnahmen unterbreitet werden.[68]

66 Vgl. *Big Data und Datenschutzrecht: Einführung, Übersicht und Webinar,* http://www.thomashelbing.com/de/big-data-datenschutzrecht-einfuehrung-uebersicht-webinar.

67 *Bundesrat will Datenschutz stärken und an technologische Entwicklung anpassen,* 15.12.2011, http://br-news.ch/bundesrat-will-datenschutz-starken-und-an-technologische-entwicklung-anpassen.

68 https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html

## SCHLUSSFOLGERUNGEN

Innovative Technologien haben oft weitreichende gesellschaftliche Folgen. Das Thema Big Data ist ein gutes Beispiel dafür. Eine Reihe von Massnahmen zum Schutz des Bürgers und zur Regulierung der Datensammlung, -speicherung und -verwendung erscheinen daher angemessen. Anzustreben ist ein Umgang mit Daten, der auf Transparenz in der gesamten Datenverarbeitungskette gegenüber deren Eigentümern basiert. Ferner werden funktionierende Kontrollmechanismen benötigt, welche die datenbearbeitenden Instanzen für den Umgang und den Schutz der Daten verantwortlich machen. Beispielsweise sollte ein Unternehmen, welches seine Pflichten im Umgang mit Daten verletzt, auch rechtliche Konsequenzen davontragen. Verschiedene Vorschläge wurden in dieser Hinsicht schon unterbreitet.[69] Drei Aspekte, die allesamt auf einem klassischen Verständnis von Eigentum basieren, stehen bei der aktuellen Debatte um einen «New Deal on Data» im Vordergrund: *Erstens* das Recht auf den Besitz von Daten. Firmen sollten eine Art (anonymes) Benutzerkonto führen, wo diese Daten gespeichert, aber auch jederzeit wieder durch den Besitzer gelöscht werden können. *Zweitens* muss der Besitzer die vollständige Kontrolle über die Verwendung der Daten haben. Sollte der Dateninhaber mit der Verwendung und/oder Handhabung der Daten nicht einverstanden sein, müsste er sie unwiderruflich löschen können. Die Zurverfügungstellung der Daten ist ein bewusster Entscheid des Inhabers. *Drittens* hat jeder Benutzer die Hoheit über seine Daten. Es ist allein seine Entscheidung, wem und für was er seine Daten zur Verfügung stellt und wann er sie abziehen und ganz löschen möchte. Diese drei Forderungen stellen das Mindestmass eines erforderlichen neuen Ansatzes zum Umgang mit Daten dar. Zugleich muss die Verwendung von grossen, anonymen Datensätzen möglich bleiben, um die Vorteile durch die Analyse solcher Datensätze zum Wohle der Allgemeinheit zu nutzen.

Um diese Veränderungen herbeizuführen, braucht es aber sowohl den Willen auf der Ebene politischer Entscheidungsträger als auch ein Umdenken seitens der Bürger. In der Schweiz sind die Reaktionen auf

69 Alex Pentland, «Reality Mining of Mobile Communications: Toward a New Deal on Data», in: *The Global Information Technology Report 2008–2009: Mobility in a Networked World* (New York: Springer, 2009), 75–80.

den NSA-Skandal gemäss Hanspeter Thür, dem eidgenössischen Datenschutzbeauftragten, allerdings noch immer milde gemessen am Ausmass der Überwachung: «Was hingegen weiterhin erstaunt, ist die grosse Indifferenz, mit der Bürger und Politiker den Skandal ertragen.»[70] Ein grösseres gesellschaftliches Interesse an der Thematik wäre angebracht. Alles deutet darauf hin, dass nicht nur der Schweizer Staat und die Schweizer Wirtschaft betroffen sind, sondern auch die Bürger direkt. Laut Thür sei es naiv zu glauben, wer nichts zu verbergen habe, habe nichts zu befürchten.[71] Trotzdem dominiert unter den Schweizerinnen und Schweizern die Apathie. Es mag zu früh sein, doch gibt es bis anhin wenig Anhaltspunkte, welche auf ein verändertes gesellschaftliches Verhalten im Umgang mit persönlichen Daten hinweisen. Gemäss Bruce Schneier, einem amerikanischen Kryptologen und selbst ein grosser Kritiker der Geheimdienste, ist jedoch genau dies der entscheidende Faktor. Solange die Menschen ihr Verhalten im Internet und ihren Umgang mit persönlichen Daten nicht ändern, werden auch die Geheimdienste und Unternehmen ihr Bestreben nach einer möglichst umfassenden Datensammlung nicht einstellen.[72] Deshalb bedarf es vor allem eines gesellschaftlichen Umdenkens, welches erlaubt, den Nutzen heutiger Technologien einzuordnen, aber auch für die Gefahren sensibilisiert zu sein. Ferner braucht es einen offenen Dialog über die Grenzen des Strebens nach Sicherheit zulasten der Freiheit und umgekehrt.

**Es gibt bis anhin wenig Anhaltspunkte, welche auf ein verändertes gesellschaftliches Verhalten im Umgang mit persönlichen Daten hinweisen.**

Big Data hat das Potenzial, in vielen Bereichen einen grossen Fortschritt zu ermöglichen. Zugleich ist das Missbrauchspotential beträchtlich. Es wäre deshalb sinnvoll, die bereits heute bestehenden Defizite im Hinblick auf die noch komplexeren Herausforderungen für den Datenschutz und den Umgang mit Daten anzugehen. Bei sämtlichen Abwägungen muss dabei der Schutz der Privatsphäre als zentraler Bestandteil der Rechte eines jeden Bürgers und als unantastbares Element

70 Thür, «Auch du bist verdächtig».

71 Ebd.

72 «Überwachung total: Die Auslöschung der Freiheit», in: *Tages-Anzeiger* (20.01.2014).

bestehen. Bis anhin sind seitens Schweizer Unternehmen keine groben Missbrauchsfälle bekannt, und die Thematik liegt für Schweizer Behörden, mit Ausnahme der obgenannten Fälle der geplanten Gesetzesrevisionen, noch in der Zukunft. Der globale Charakter der Informationsgesellschaft lässt allerdings eine auf Staatsgrenzen beschränkte Betrachtungsweise als kurzsichtig erscheinen. Zukunftsorientierte Konzepte im Hinblick auf die rechtlichen, politischen und gesellschaftlichen Herausforderungen im Umgang mit Daten, dem Datenschutz und der Privatsphäre müssen deshalb vor allem auch auf internationaler Ebene angegangen werden.

Grundsätzlich hat die Snowden-Zäsur auch in der Schweiz zu einer gewissen Sensibilisierung der breiten Öffentlichkeit und politischer Kreise geführt. Diesen Diskurs gilt es zu intensivieren. Dabei sollte ein Mittelweg zwischen der Festigung der inneren und äusseren Sicherheit einerseits und der Wahrung der Bürgerrechte andererseits als Orientierung dienen.