Maximilian Sönke Wolf

Big Data und Innere Sicherheit

Grundrechtseingriffe durch die computergestützte Auswertung öffentlich zugänglicher Quellen im Internet zu Sicherheitszwecken

Tectum

Big Data und Innere Sicherheit.
Grundrechtseingriffe durch die computergestützte Auswertung öffentlich zugänglicher Quellen im Internet zu Sicherheitszwecken

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der rechtswissenschaftlichen Fakultät

der Albert-Ludwigs-Universität

Freiburg i. Br.

vorgelegt von

Maximilian Sönke Wolf

2015

Dekan: Prof. Dr. Matthias Jestaedt

Erstgutachter: Prof. Dr. Ralf Poscher
Zweitgutachter: Prof. Dr. Jens-Peter Schneider

Dissertationsort: Freiburg im Breisgau

Datum der Disputation: 13.05.2015

Erscheinungsjahr: 2015

Maximilian Sönke Wolf

Big Data und Innere Sicherheit

Maximilian Sönke Wolf

Big Data und Innere Sicherheit

Grundrechtseingriffe durch die computergestützte Auswertung öffentlich zugänglicher Quellen im Internet zu Sicherheitszwecken

Tectum Verlag

Maximilian Sönke Wolf

Big Data und Innere Sicherheit.
Grundrechtseingriffe durch die computergestützte Auswertung öffentlich zugänglicher Quellen im Internet zu Sicherheitszwecken

Zugl. Diss. Albert-Ludwigs-Universität Freiburg 2015

ISBN: 978-3-8288-6256-2

(Dieser Titel ist zugleich als gedrucktes Buch unter
der ISBN 978-3-8288-3600-6 im Tectum Verlag erschienen.)

Besuchen Sie uns im Internet
www.tectum-verlag.de

Bibliografische Informationen der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Angaben sind im Internet über http://dnb.ddb.de abrufbar.

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2015 von der Juristischen Fakultät der Albert-Ludwigs-Universität Freiburg als Dissertation angenommen. Sie entstand während meiner Zeit als Akademischer Mitarbeiter des Kompetenznetzwerkes für das Recht der zivilen Sicherheit in Europa (KORSE).

Mein Dank gilt Herrn Prof. Dr. Ralf Poscher für die Betreuung der Arbeit sowie Herrn Prof. Dr. Jens-Peter Schneider für die rasche Erstellung des Zweitgutachtens.

Besonderen Dank möchte ich zudem an das Bundesministerium für Bildung und Forschung für die Finanzierung des Forschungsvorhabens KORSE richten sowie an Herrn Prof. Dr. Martin Hochhuth für die Leitung des Projektes und seine stete Gesprächs- und Motivationsbereitschaft.

Freiburg, Juni 2015 Maximilian Sönke Wolf

Inhaltsverzeichnis

Einleitung

A. Problemstellung

Als im Jahr 1983 das Volkszählungsurteil gesprochen wurde, waren es noch die klassischen Massenmedien wie Rundfunk und Presse, die die wesentliche Rolle bei der Vermittlung von Informationen an die Gesellschaft spielten. Weder waren das Internet in seiner heutigen Struktur noch Suchmaschinen oder die sozialen Medien bekannt. Doch bereits damals sorgte sich die Rechtswissenschaft, die fortschreitende Datenverarbeitung könne zur informationellen Durchleuchtung des Bürgers führen, ihn gar zum gläsernen Menschen werden lassen.[1] Knapp zwanzig Jahre nach dem Volkszählungsurteil wurden mit Google und Facebook Unternehmen gegründet, die die Welt neben zahlreichen anderen, parallel verlaufenden Prozessen in ein neues digitales Zeitalter führten; das der ubiquitären Digitalisierung oder einfacher: Big Data.

Während der gläserne Mensch nun keine Fiktion mehr ist, scheint mit der Enthüllung des globalen Überwachungsprogrammes der NSA im Jahr 2013 auch die informationelle Durchleuchtung durch den Staat kein reines Szenario mehr zu sein. Insofern könnte ein ernüchterndes Fazit aus den ersten Jahrzehnten datenschutzrechtlicher Bemühungen gezogen werden. Da die globalen Datennetze durch einzelne Staaten nicht mehr kontrollierbar seien, werden schon die Rufe lauter, der Privatsphärenschutz sei gar ein überkommenes Relikt, das in der digitalen Zukunft keine Geltung mehr beanspruchen könne.[2] Mit dem Big Data Zeitalter sei ein weiteres angebrochen, das der Post-Privacy. Durchaus fällt es schwer, sich des Eindrucks zu erwehren, dass die Privatheit in der Gesellschaft an Stellenwert eingebüßt hat. Was einst als typischerweise privat galt, wird heute oft freizügig in sozialen Online-Netzwerken der Allgemeinheit zugänglich gemacht. Die Grenze zwischen Privatheit und Öffentlichkeit scheint sich aufzulösen. Doch diese Entwicklung bedeutet nicht, dass der Datenschutz zum Scheitern verurteilt ist. Das informationelle Selbstbestimmungsrecht kann auf den gesellschaftlichen Wandel reagieren, denn es geht über den Schutz der Privatsphäre weit hinaus. Das BVerfG entschied, dass der Schutz des Einzelnen nicht ende, wenn er sich in die Öffentlichkeit begebe,

---

1 *Haft*, NJW 1979, S. 1194, 1197.

2 Vgl. *Heller*, Post-Privacy, München 2011.

sodass auch die Videoüberwachung im öffentlichen Raum und die automatisierte Kennzeichenerfassung einen Eingriff in das informationelle Selbstbestimmungsrecht darstellten.[3] Die Erhebung personenbezogener Informationen in öffentlich zugänglichen Bereichen bleibt demnach rechtfertigungsbedürftig.

Ein so weitgehender Schutz gilt für die frei zugänglichen Räume des Internets hingegen nicht. Zwar schütze das Recht auf informationelle Selbstbestimmung sämtliche personenbezogenen Informationen, sodass es belanglose Daten nicht mehr gebe.[4] Dennoch greife die Erhebung allgemein zugänglicher Netzinhalte im Regelfall nicht in das informationelle Selbstbestimmungsrecht ein.[5] Damit erklärt das BVerfG personenbezogene Informationen in öffentlich zugänglichen Internetquellen zwar nicht für gänzlich schutzlos, denn zumindest ein systematisches Zusammentragen vieler Daten bedürfe weiterhin einer gesetzlichen Grundlage.[6] Dennoch divergiert die rechtliche Bewertung staatlicher Informationserhebungen innerhalb und außerhalb des virtuellen Raumes. Diese Diskrepanz könnte damit begründet werden, dass die Gefährdungen, die staatliche Ermittlungen in frei zugänglichen Bereichen des Internets für den Einzelnen hervorrufen, nicht größer sind als jene Gefährdungen, die durch die Beobachtung von gewöhnlichen Polizeistreifen hervorgerufen werden. Denn letztere stellen nach allgemeiner Auffassung ebenfalls keinen Eingriff in die Grundrechte dar.[7] Eine solche Gleichbehandlung erscheint jedoch fragwürdig. Die Masse der frei zugänglichen personenbezogenen Informationen hat sich mit dem Aufstieg der sozialen Medien im vergangenen Jahrzehnt erheblich erhöht. Die Beobachtung der sozialen Online-Netzwerke, Weblogs und Multimediaplattformen lässt Einblicke in das Leben vieler Bürger zu, die keine Polizeistreife gewinnen könnte. Darüber hinaus ermöglichen moderne Verfahren der Datenanalyse eine weitgehend automatisierte Filterung der allgemein zugänglichen Inhalte in solche sicherheitsrelevanter und -irrelevanter Art. Mittels Big Data Anwendungen können die frei zugänglichen Datenströme der sozialen Medien automatisiert angezapft, deren Inhalte gespeichert, analysiert und anschließend

3 BVerfGE 120, 378, 399; 122, 342, 368.

4 BVerfGE 65, 1, 45.

5 BVerfGE 120, 274, 344f.

6 BVerfGE 120, 274, 345.

7 Statt aller *Gusy*, Polizei- und Ordnungsrecht, Rn. 165.

verwertet werden. Persönlichkeits- und Bewegungsprofile können aus den gewonnen Informationen erstellt werden, frei zugängliche Kommunikationsströme auf rechtswidrige Inhalte durchsucht und Netzwerke extremistischer Gruppierungen aufgedeckt werden. Die Überwachung des virtuellen öffentlichen Raumes gestaltet sich aufgrund der ungeahnten technischen Möglichkeiten einfacher als jene des reellen Raumes. Zugleich besteht ein nicht abzustreitendes Bedürfnis der Sicherheitsbehörden, die im Internet zugänglichen Informationen für ihre Zwecke zu nutzen. Dies resultiert daraus, dass das Internet eine besonders ergiebige Informationsquelle ist und zugleich seit seiner Schaffung auch für illegitime Aktivitäten genutzt wird. Soziale Medien erlauben die Streuung von Informationen an unbeschränkte Empfängerkreise und werden daher nicht nur von etablierten politischen Gruppierungen, sondern auch für religiöse und politische Propaganda in extremistischen Kreisen genutzt. Sie sind ein Nährboden für Islamismus sowie Rechts- und Linksradikalismus,[8] weswegen ihre systematische Beobachtung die innere Sicherheit fördern würde.

Die vorliegende Arbeit untersucht, ob und in welche Grundrechte die Nutzung von Technologien eingreift, die zur automatisierten und teilweise flächendeckenden Auswertung öffentlich zugänglicher Inhalte im Internet eingesetzt werden können. Im Fokus der Untersuchung steht – für staatliche Überwachungsmaßnahmen charakteristisch – das Recht auf freie Entfaltung der Persönlichkeit, insbesondere in seiner Ausformung als Recht auf informationelle Selbstbestimmung. Die Untersuchung bleibt aber nicht auf dieses Grundrecht beschränkt, sondern widmet sich weiteren Freiheitsrechten, deren Wahrnehmung im virtuellen Raum durch eine umfassende Überwachung gefährdet ist. Die Untersuchung konzentriert sich auf Big Data Analyseverfahren, da diese eine weitaus raumgreifendere Überwachung als die manuelle Beobachtung der Inhalte im Netz ermöglichen und damit neuartige Gefährdungen für die individuelle Entfaltung hervorrufen. Anders als die manuelle Ermittlung im Netz[9] ist die automatisierte Überwachung von Inhalten mittels moderner Erhebungs-

---

8 Vgl. etwa *Bundesamt für Verfassungsschutz/Landesbehörden für Verfassungsschutz*, Salafistische Bestrebungen in Deutschland, S. 13f.; *Bundesamt für Verfassungsschutz*, Rechtsextremisten und ihr Auftreten im Internet, S. 7f.

9 Zu dieser vgl. *Böckenförde*, Die Ermittlung im Netz, Tübingen 2003 und zuletzt *Oermann/Staben*, Der Staat 2013, S. 630ff.

und Analyseverfahren noch nicht Gegenstand rechtswissenschaftlicher Untersuchungen geworden. Die Einschränkung des Untersuchungsgegenstandes auf öffentlich zugängliche Daten erfolgt, da ihre einfache Verfügbarkeit sie zu praktisch besonders relevanten Quellen in der Arbeit der Sicherheitsbehörden macht. Andererseits wirft ihre stiefmütterliche rechtswissenschaftliche Behandlung die Fragen auf, ob und warum sie überhaupt des Schutzes der Rechtsordnung bedürfen. Zugleich sind die öffentlich zugänglichen Quellen geeignet, das besondere Gefährdungspotential zu präsentieren, das durch die staatliche Nutzung von Big Data Anwendungen hervorgerufen wird. Denn während die manuelle Erhebung *vertraulicher* Daten in das informationelle Selbstbestimmungsrecht eingreift, sind frei zugängliche Netzinhalte nicht in gleicher Weise geschützt. Den Analysefähigkeiten von Big Data könnte damit eine entscheidende Rolle bei der rechtlichen Bewertung der Überwachung öffentlich zugänglicher Bereiche im Netz zukommen.

Zur Beantwortung der leitenden Fragestellungen bedarf es einerseits der Untersuchung der Potentiale, die die Nutzung der öffentlichen Räume des Internets für die innere und äußere Entfaltung der Persönlichkeit bietet. Mit der steten digitalen Durchdringung aller Lebensbereiche verlagert sich auch die Wahrnehmung der grundrechtlich geschützten Freiheiten sukzessive in den virtuellen Raum. Andererseits müssen die Gefährdungen ermittelt werden, die deren computergestützte staatliche Überwachung mit sich bringt. Mag der Gegenstand der Arbeit demnach rein manuelle Überwachungsmaßnahmen auch ausklammern, so ist dennoch zu erwarten, dass die Untersuchungsergebnisse auch zu deren rechtlicher Beurteilung fruchtbar gemacht werden können. Gerade die Unterschiede zwischen der manuellen Überwachung und jener computergestützten vermögen die neuartigen Gefahrenpotentiale aufzudecken. Der Gegenstand der vorliegenden Arbeit ist zudem auf das Verhältnis zwischen dem Staat und dem über das Internet kommunizierenden Bürger beschränkt. Inwieweit die Informationserhebung bei der Arbeit der Sicherheitsbehörden in die Grundrechte der Dienstanbieter eingreift, etwa in deren Berufsfreiheit oder die Eigentumsgarantie,[10] bedürfte einer eigenständigen Untersuchung.

[10] Hierzu etwa *Henrichs/Wilhelm*, in: Kriminalistik 2010, S. 218ff.

B. Gang der Untersuchung

Zunächst wird im Rahmen einer Realanalyse im *ersten Teil* eine Einführung in die jüngsten digitalen Entwicklungen gegeben, die in der Fachliteratur und der Presse unter dem Schlagwort Big Data behandelt werden. Dies dient der Sensibilisierung für die Potentiale und Gefährdungen, die mit diesen Entwicklungen für die Persönlichkeitsentfaltung des Bürgers einhergehen. Anschließend werden die sozialen Medien vorgestellt, die die bedeutendste frei zugängliche Informationsquelle des Internets für die Arbeit der Sicherheitsbehörden darstellen. Daraufhin wird die praktische Relevanz der staatlichen Beobachtung öffentlich zugänglicher Quellen im Internet dargestellt. Dabei werden aktuelle und potentielle Anwendungsfelder in der präventiven und repressiven Polizeiarbeit sowie im Gefahrenvorfeld skizziert. Der erste Teil der Untersuchung schließt mit einer exemplarischen Vorstellung verschiedener Big Data Anwendungen zur Überwachung der öffentlich zugänglichen Quellen ab. Hierbei kann nur ein begrenzter Ausschnitt aus dem weiten Feld der sich stets weiterentwickelnden Technologien dargestellt werden. Doch genügt dieser Ausschnitt dazu, die wesentlichen Charakteristika der Big Data Anwendungen und der durch sie hervorgerufenen Gefahren zu veranschaulichen.

Der *zweite Teil* analysiert zunächst, was das BVerfG unter öffentlich zugänglichen Daten im Internet versteht, um sodann aufzuzeigen, welche Konsequenzen eine Kategorisierung als öffentlich zugänglich für die rechtliche Beurteilung staatlicher Informationserhebungen hat. Anschließend wird die Fülle der personenbezogenen Daten in den sozialen Medien den öffentlichen bzw. nicht öffentlichen Quellen zugeordnet. Da das BVerfG die Eingriffsqualität von Informationserhebungen teilweise auch in solchen Bereichen im Internet verneint, die nicht öffentlich zugänglich sind, wird der Untersuchungsgegenstand zum Schluss des zweiten Teils um einen exkursiven Teil erweitert.

Im *dritten Teil* wird untersucht, welche Grundrechte vor den Gefährdungen Schutz bieten, die mit einer staatlichen Überwachung der sozialen Medien einhergehen. Innerhalb dessen wird das spezifische Gefährdungspotential der Nutzung von Big Data Anwendungen herausgearbeitet und zugleich analysiert, welchen Einfluss die öffentliche Zugänglichkeit der Daten auf den grundrechtlichen Schutz hat. Insbesondere der Schutzgehalt des Rechts auf freie Entfaltung der Persönlichkeit und seiner

Derivate wird unter Reflexion seiner rechtswissenschaftlichen und verfassungsgerichtlichen Herleitung näher untersucht. Daneben stehen die Gewährleistungen der Kommunikationsfreiheiten des Grundgesetzes im Fokus des dritten Teils.

In enger Anbindung zum vorausgehenden Abschnitt erörtert der *vierte Teil* der Untersuchung, unter welchen Voraussetzungen das ermittelte Gefährdungspotential zu einem Grundrechtseingriff führt. Unabdingbar ist dabei eine Befassung mit dem Eingriffsbegriff und dessen Implikationen für die grundrechtliche Beurteilung der einschüchternden Wirkung staatlicher Überwachungsmaßnahmen. Dazu werden verschiedene Konzepte aus Literatur und Rechtsprechung zur Behandlung psychisch vermittelter, faktischer Beeinträchtigungen hinterfragt, kritisch gewürdigt und auf die Problemstellung angewandt.

Im *fünften Teil* wird untersucht, inwieweit den negativen Seiten der Freiheitsrechte ein spezifischer Informationsschutz entnommen werden kann. Exemplarisch befasst sich die Untersuchung mit den negativen Gewährleistungen der Meinungsfreiheit sowie der Religionsfreiheit. Die enge Verflechtung der Schutzgehalte mit den sie beschränkenden Maßnahmen erfordert ein eigenständiges Kapitel außerhalb der klassischen Trennung von Schutzbereich und Eingriff.

Die Untersuchung schließt im *sechsten Teil* mit einer Betrachtung des Konkurrenzverhältnisses der betroffenen Grundrechte ab.

C. Begriffsbestimmungen

Die den Untersuchungstitel prägenden Ausdrücke Big Data und innere Sicherheit bedürfen der näheren Betrachtung. Beide Begriffe werden in Fachliteratur, Presse und Politik häufig verwendet, bisweilen auch gemeinsam. Doch bleiben ihre Bedeutungen oftmals vage. Grund hierfür mag sein, dass *Big Data* nicht technisch normiert und die *innere Sicherheit* nicht wörtlich im Grundgesetz zu finden ist. Da sie den Untersuchungsgegenstand umschreiben, sollen sie aber hinreichend präzisiert werden. Erschwert wird dies, da beide Begriffe bereits im Ursprung auf ein offenes Verständnis angelegt sind. Andererseits macht sie dies insofern für diese

Untersuchung attraktiv, als der Gegenstand bereits durch die Beschränkung auf *öffentlich zugängliche Quellen*[11] erheblich begrenzt ist.

I. Big Data

Der Ausdruck Big Data beschreibt ein Phänomen, das im engen Zusammenhang zur stetig fortschreitenden, ubiquitären Digitalisierung steht. Die vielfältigen Erscheinungsformen dieses Phänomens sind in unterschiedlicher Stärke in verschiedenen Kontexten zu beobachten. Hingegen können sie schwerlich durch eine abstrakte Definition erfasst werden. Dies mag erklären, warum bei der Verwendung des Begriffes Big Data häufig auf eine genauere Erläuterung desselben verzichtet wird. Aufgrund seiner vagen Bedeutung wird er denn auch als *Schlagwort* für eine Vielzahl neuer Technologien verstanden, die der *Analyse besonders großer Datenmengen* dienen.[12] In der informationstechnologischen Literatur finden sich vereinzelt *Kriterien*, anhand derer beurteilt wird, wann eine bestimmte Datenmenge Big Data zuzuordnen ist. Dabei wird auf den Umfang, die Komplexität und die Geschwindigkeit des Aufkommens der Daten innerhalb einer Datensammlung abgestellt.[13] Andere Ansätze bringen zum Ausdruck, dass es sich um Datensätze handelt, die mit herkömmlichen Speicher- und Analysemethoden nicht mehr erfassbar sind,[14] und betonen damit den Eintritt in ein neues Stadium der Datenverarbeitung.

In dieser Untersuchung werden die Potentiale und Gefahren betrachtet, die die Digitalisierung zahlreicher Lebensbereiche und deren sukzessive Verlagerung in die öffentlich zugänglichen Bereiche des Internets mit sich bringt. Das Kunstwort Big Data beschreibt neben anderen auch dieses Phänomen.[15] Der Bundesverband Informationswirtschaft fasst Big Data

---

11 Der Begriff der öffentlich zugänglichen Quellen wird zu Beginn der rechtlichen Analyse genauer betrachtet, dazu unten S. 69ff.

12 *Lerman*, Stan. L. Rev. 66 (2013), S. 55 bei Fn. 1.

13 Sog. *three v´s*: volume, variety, velocity, vgl. *TechAmerica*, Demystifying Big Data, S. 10 f.; *Bundesverband Informationswirtschaft* (Hrsg.), Big Data im Praxiseinsatz, S. 19; nach dem Bundesverband Informationswirtschaft sind die Daten, die Facebook täglich speichert, beispielhaft für die Erfüllung dieser Kriterien, vgl. Big Data im Praxiseinsatz, S. 7 bei Fn. 1.

14 *Manyika* et al., Big data, S. 11; vgl. auch *Smith* et al., Big Data Privacy Issues, S. 1.

15 *Bundesverband Informationswirtschaft* (Hrsg.), Big Data im Praxiseinsatz, S. 20.

pragmatisch als Vorgang der „Analyse großer Datenmengen aus vielfältigen Quellen in hoher Geschwindigkeit mit dem Ziel, wirtschaftlichen Nutzen zu erzeugen", zusammen.[16] Wird dieses Verständnis aus dem betriebswirtschaftlichen Zusammenhang gelöst und auf die Aufgabenbereiche der Sicherheitsbehörden übertragen, ist es einerseits flexibel genug, die für die innere Sicherheit relevanten Auswertungsmethoden zu erfassen. Andererseits genügt es den funktionalen Anforderungen, die an eine Begriffsklärung in dieser Untersuchung zu stellen sind und zugleich knüpft es an die Kriterien der informationstechnischen Literatur[17] an. In Abgrenzung zur manuellen Aufklärung des Internets stehen im Fokus dieser Untersuchung demnach *automatisierte Anwendungen, die große Datenmengen aus den vielfältigen öffentlich zugänglichen Quellen des Internets in hoher Geschwindigkeit analysieren, um einen Nutzen für die Arbeit der Sicherheitsbehörden zu generieren*.[18] Für die vorliegende Untersuchung bringt eine differenziertere Ausarbeitung des Begriffes Big Data, so sie denn überhaupt möglich ist, keinen Erkenntnisgewinn. Denn für die Potentiale und Gefahren, die die ubiquitäre Digitalisierung mit sich bringt, ist es nicht entscheidend, ob eine Datensammlung in Umfang oder Komplexität eine wie auch immer definierte Grenze überschreitet oder nicht. Wohl aber ist es entscheidend, das Phänomen Big Data in seinen praktischen Auswirkungen zu begreifen. Auf diese wird nach einer Erläuterung des Begriffes der inneren Sicherheit eingegangen werden.[19]

II. Innere Sicherheit

Der Begriff der inneren Sicherheit ist ebenfalls unbestimmt und offen, wenn er aus dem staatsrechtlichen Zusammenhang gelöst und als eine politische Größe im Kontrast zu anderen Zielsetzungen verstanden wird.[20] Dann beschreibt er einen erstrebenswerten Idealzustand,[21] dessen inhaltliche Ausfüllung von den Idealen des jeweiligen Betrachters abhängig

---

16 Big Data im Praxiseinsatz, S. 7.

17 Vgl. Fn. 13.

18 Im Folgenden werden diese Anwendungen auch als Big Data Anwendungen bezeichnet.

19 Siehe insbesondere die S. 25ff. und im sicherheitsrechtlichen Kontext S. 36ff.

20 Kritisch zum Nutzen des Begriffes daher *Kniesel*, ZRP 1996, S. 482, 485.

21 *Meyer*, Terror und Innere Sicherheit, S. 12.

ist.[22] Zuweilen wird der Begriff der inneren Sicherheit daher als beliebig auffüllbares Schlagwort kritisiert.[23]

Das *staatsrechtliche Verständnis* hingegen beschreibt einen verfassungsrechtlich vorgegeben Aufgabenbereich des Staates.[24] Dieser Bereich steckt den Rahmen jener Zwecke ab, auf die die Auswertung öffentlich zugänglicher Quellen im Internet in dieser Untersuchung thematisch begrenzt ist. Der Aufgabenbereich der inneren Sicherheit kann zunächst in Abgrenzung zur äußeren Sicherheit verstanden werden.[25] Das Handlungsfeld der äußeren Sicherheit beschreibt die Abwehr von Gefahren, die dem Staat von außen durch feindliche Mächte drohen.[26] Infolgedessen ist die Verteidigung einer ihrer Zentralbegriffe.[27] Die Streitkräfte, denen die Gewährleistung der äußeren Sicherheit nach Art. 87a GG zugewiesen ist, sind daher im Regelfall kein Akteur im Aufgabenbereich der inneren Sicherheit.[28]

Die innere Sicherheit wendet sich gegen die Gefahren, die aus dem Inneren des Staates und demnach aus der Gesellschaft heraus für die individuellen und überindividuellen Rechtsgüter drohen. Zu diesen Gefahren sind sämtliche Erscheinungsformen der Kriminalität zu zählen sowie die Bedrohungen für den Bestand und die Funktionsfähigkeit des demokratischen Rechtsstaats.[29] Dementsprechend erfolgt die Gewährleistung der inneren Sicherheit vornehmlich durch die Bekämpfung von Kriminalität und Terrorismus mit präventiven und repressiven Mitteln, aber auch durch sämtliche Tätigkeiten der Vollzugspolizei.[30] Staatliche Akteure in

---

22 Vgl. *Schlögel*, Bundesverfassungsgericht im Politikfeld Innere Sicherheit, S. 16.

23 *Kniesel*, ZRP 1996, S. 482, 485.

24 Vgl. *Pitschas*, JZ 1993, S. 857, 858; *Kniesel*, ZRP 1996, S. 482: „Aufgabenkonglomerat".

25 Zur Problematik dieser Abgrenzung aufgrund moderner Gefahrenlagen vgl. *Depenheuer*, in: Maunz/Dürig, Art. 87a Rn. 12ff.

26 *Meyer*, Terror und Innere Sicherheit, S. 13f.

27 *Götz*, HStR IV, S. 679f.

28 BVerfG NVwZ 2012, S. 1239, 1241: „Die Verfassung begrenzt einen Streitkräfteeinsatz im Inneren in bewusster Entscheidung auf äußerste Ausnahmefälle"; vgl. auch *Dependeuer*, in: Maunz/Dürig, Art. 87a Rn. 12; *Götz*, HStR IV, S. 689ff.; zu beachten sind jedoch die gewichtigen Ausnahmen des Art. 87a II GG i.V.m. Art. 35 GG (Katastrophenschutz) und i.V.m. Art. 91 GG (innere Unruhen), vgl. dazu BVerfG NVwZ 2012, S. 1239, 1241ff. u. *Maunz*, in: Maunz/Dürig, Art. 35 Rn. 15.

29 *Götz*, HStR IV, S. 672.

30 Dazu und zu weiteren Aufgabenfeldern *Götz*, HStR IV, S. 673ff.

dem Aufgabenfeld der inneren Sicherheit sind neben den Polizeien des Bundes und der Länder die Strafverfolgungsbehörden und die Nachrichtendienste.[31] Deren gesetzlich zugewiesenen Aufgaben stecken den Bereich ab, in denen die Nutzung von Big Data Anwendungen zur Auswertung öffentlich zugänglicher Quellen im Internet untersucht wird.

[31] *Schwabenbauer*, Heimliche Grundrechtseingriffe, S. 17ff.; *Meyer*, Terror und Innere Sicherheit, S. 17.

Teil 1: Realanalyse

A. Das Big Data Zeitalter

Der den Untersuchungstitel prägende Ausdruck Big Data ist ein immer mehr in Mode kommender Begriff. Big Data steht plakativ für gewaltige Massen von Daten, die heutzutage auf allen Ebenen – von Behörden bis Wirtschaftsunternehmen – gesammelt werden. Unternehmen erheben Milliarden von Einzelinformationen über ihre Kunden, automatische Sensoren wie GPS-Sender generieren sie eigenständig und in Web 2.0 Anwendungen wie sozialen Netzwerken werden sie von jedermann für jedermann freiwillig zur Verfügung gestellt.[32] Die Menge der global vorhandenen Daten wird täglich größer und soll sich bis in das Jahr 2020 vervierzigfachen.[33] Moderne Big Data Technologien helfen dabei, die riesigen Datenbestände computergestützt auszuwerten und die in ihnen enthaltenen Informationen in Bezug zueinander zusetzen. Sie zielen darauf ab, einen positiven Nutzen aus den vielfältigen und unstrukturierten Daten zu ziehen, die den jeweiligen Akteuren zur Verfügung stehen.[34] Dort, wo die konventionelle Datenverarbeitung an ihre Grenzen stößt, setzt Big Data ein.[35] Der spezifische Wert von Big Data liegt in der Masse an Daten, aus denen sich Muster und Trends ermitteln lassen. Hilfreich sollen Big Data Technologien in zahlreichen Lebens- und Wirtschaftsbereichen sein, etwa in der Medizin, um die Echtzeiterkennung von Grippeepidemien zu ermöglichen[36] oder um maßgeschneiderte Behandlungsmethoden zu berechnen.[37] In der Wirtschaft sollen sie nicht nur die Bedarfsplanungen vereinfachen[38], sondern als vierter Produktionsfaktor neben Arbeit, Kapital

---

32 *Manyika* et al., Big data, S. 4.

33 *Manyika* et al., Big data, S. 16 m.w.N.

34 *Kempf*, in: Bundesverband Informationswirtschaft (Hrsg.), Big Data im Praxiseinsatz, S. 5.

35 *Bundesverband Informationswirtschaft* (Hrsg.), Big Data im Praxiseinsatz, S. 8.

36 *Mayer-Schönberger/Cukier*, Big Data: A Revolution, S. 2f.

37 *Der Spiegel*, vom 16.07.2013, abrufbar unter: http://www.spiegel.de/wissenschaft/medizin/big-data-wundermittel-auch-fuer-die-medizin-a-911333.html.

38 *Die Zeit*, vom 03.01.2013, abrufbar unter: http://www.zeit.de/2013/02/Big-Data.

und Rohstoffe treten.[39] Selbst zur Vorhersage von Wahlergebnissen scheint Big Data dienlich zu sein.[40]

Zur exponentiell wachsenden Datenflut[41] trägt dabei jeder Einzelne – oft unbewusst – bei. Sei es durch die Standortangaben seines Mobiltelefons, Suchwortanfragen bei Google, Kreditkartenabbuchungen, Payback-Kundenkarten, mittels Facebook-Einträgen oder der Nutzung intelligenter Stromzähler.[42] Das aufkommende Internet der Dinge, also die Verbindung von Objekten mit dem Internet[43], scheint diese Entwicklung noch zu verstärken.[44] Doch nicht nur die private Wirtschaft partizipiert an Big Data. Auch die öffentliche Hand nimmt durch eine fortschreitende Digitalisierung der Verwaltungsarbeit in zahlreichen Segmenten an der aufgezeigten Entwicklung teil. Beispielhaft hierfür ist die Einführung elektronischer Akten (sog. E-Akten) in Sachbereichen wie Steuern[45] und Arbeit[46], aber auch in der Kommunalverwaltung.[47] Sorgen ob der Gewährleistung ihrer Privatsphäre ruft diese Entwicklung auf den genannten Sachgebieten bei den Bürgern meist nur begrenzt hervor. Schlagartig ändert sich dies, wenn Datensammlungen in staatlicher Hand zu Sicherheitszwecken geschaffen und genutzt werden. Zu solchen zählen etwa polizeiliche Datenverbünde wie das polizeiliche Auskunftssystem Baden-Württembergs (POLAS) mit über fünf Millionen Falldaten[48] oder dessen Äquivalent INPOL auf Bundesebene. Dieses nach § 11 BKAG beim Bundeskriminalamt geführte, digitale Informationssystem enthält in verschiedenen Dateien unterschiedlichste Informationen zu Straftaten und Straf-

---

39 *Bundesverband Informationswirtschaft* (Hrsg.), Big Data im Praxiseinsatz, S. 7.

40 *Jackson*, Internal Auditor 2/2013, S. 34, 35.

41 *Manyika* et al., Big data, S. 26.

42 Fiktives Beispiel bei *Lerman*, Stan. L. Rev. 66 (2013), S. 55, 58.

43 Zu diesem vgl. *Miorandi* et al., Ad Hoc Networks 10 (2012), S. 1497ff.

44 *Manyika* et al., Big data, S. 25.

45 Zur elektronischen Steuerakte in Baden-Württemberg vgl. LT-Drs. BW 13/4947, S. 3.

46 Zur Einführung der E-Akte vgl. *Focus*, vom 26.06.2012, abrufbar unter: http://www.focus.de/politik/deutschland/berge-von-papier-bundesagentur-fuer-arbeit-fuehrt-elektronische-akte-ein_aid_772753.html.

47 Z.B. Berliner Senatsbeschluss S-3831/2011.

48 Zahlen nach *Wolf/Stephan/Deger*, PolizeiG BW, § 38 Rn. 1.

tätern. So existiert u.a. eine Datei zur Erfassung sämtlicher Rauschgiftdelikte mit einem Umfang von ca. 1,5 Millionen Datensätzen[49] sowie der sog. Kriminalaktennachweis, der personenbezogene Daten von Tätern und Beschuldigten in 4,5 Millionen Datensätzen enthält.[50] Die staatlichen Datenverbünde kommen in ihrem Umfang zwar nicht an jene der Global Player wie Google oder Facebook heran, gleichwohl bleibt die öffentliche Hand vom Big Data Zeitalter nicht unberührt. Polizeibehörden in den USA und Großbritannien nutzen Big Data Technologien bereits gezielt zu Sicherheitszwecken im Vorfeld von Gefahren. Das sog. Predictive Policing verspricht, mittels der Nutzung von Data Mining Software[51] die Masse der durch Polizeibehörden gesammelten Daten derart analysieren zu können, dass das Auftreten künftiger Kriminalität präzise vorhergesagt werden kann.[52] Aus digitalisierten historischen und aktuellen Fallakten werden die relevanten Fallgrunddaten[53] entnommen und diese gemeinsam mit anderen gesammelten Daten, beispielsweise über Notrufe, Haftbefehle, Umgebungsinformationen[54] und sogar Wetterberichte, analysiert, um Kriminalitätsmuster zu erkennen und um Orte und Zeitpunkte vorherzusagen, an denen mit hoher Wahrscheinlichkeit zukünftige Straftaten stattfinden.[55] Vorhersagen über zu erwartende Kriminalität erfolgen dabei nicht manuell, sondern über die Anwendung von Computer-Algorithmen, die Muster in den gesammelten Daten erkennen und je nach Bedeutung für die Vorhersage gewichten.[56] Letztlich soll mit Hilfe von Big Data Technologien die Polizei „vor dem Täter, den es dann nicht mehr gäbe,

---

49 Zahlen nach *Lisken/Denninger/Petri*, Handbuch des Polizeirechts, S. 746 Rn. 82.

50 *Lisken/Denninger/Petri*, Handbuch des Polizeirechts, S. 748 Rn. 86.

51 Software, die unbekanntes, aber potentiell nützliches Wissen aus großen Datensammlungen extrahiert und dabei insbesondere Gesetzmäßigkeiten und verborgene Zusammenhänge aufdeckt, vgl. *Ester/Sander*, Knowledge Discovery in Databases, S. 4; zur Begrifflichkeit siehe *Duden online*, Data-Mining: Bedeutung, Rechtschreibung, Grammatik, Herkunft.

52 *Ferguson*, Emory Law Journal 2012, S. 259, 261.

53 Etwa Art der Straftat sowie Ort und Zeit des Auftretens; Terminologie nach *Wirth* (Hrsg.), Kriminalistik-Lexikon, S. 297.

54 Beispielsweise Daten über die soziale Struktur bestimmter Orte.

55 *Ferguson,* Emory Law Journal 2012, S. 259, 265f.

56 *Ferguson*, Emory Law Journal 2012, S. 259, 266.

am Tatort sein“[57].[58] Noch in erheblicherem Maße spiegelt sich die Entwicklung, dass Big Data und staatliche Sicherheitsmaßnahmen in Zukunft kaum zu trennen sein werden, in den Abhörprogrammen ausländischer Geheimdienste wie *Prism* und *Tempora* wieder, die im Jahr 2013 publik wurden. Der britische Geheimdienst etwa greift auf weite Teile der über das Internet geleiteten Telekommunikation zu, indem er direkt die transatlantischen Datenverbindungen anzapft, also Glasfaserkabel, die große Teile des globalen Datenverkehrs leiten.[59] Theoretisch kann auf diese Weise täglich ein Datenvolumen von über 20 Petabyte[60] erhoben und auf nachrichtendienstlich verwertbare Informationen durchsucht werden.[61] Die erhobenen Datenmassen, die geradezu beispielhaft für Big Data sind, umfassen dabei persönlichste Informationen wie E-Mails, Sprachtelefonien, Nachrichten in sozialen Netzwerken etc.[62] Anders als bei *Tempora* wurde beim US-amerikanischen Überwachungsprogramm *Prism* deutlich, dass eine Trennung von Big Data in privater und öffentlicher Hand kaum mehr gewährleistet ist. Medienberichten zufolge hat der US-amerikanische Geheimdienst direkten Zugriff auf die Server der größten Anbieter sozialer Medien wie Apple, Microsoft, Google und Facebook und kann demnach auf deren Datensammlungen zu Sicherheitszwecken unmittelbar zugreifen.[63] Gemeinsam ist sämtlichen Akteuren, die Big Data Technologien in der Wirtschaft, der Medizin oder eben zur staatlichen Sicherheitsarbeit nutzen, dass sie sich ähnlicher Analysemethoden zur Auswertung der manuell nicht mehr handhabbaren Datenmassen bedienen.

B. Öffentlich zugängliche Datenquellen im Internet

Die vorliegende Untersuchung behandelt ausschließlich solche Datenquellen im Internet, die für jedermann frei zugänglich sind, also öffentlich

---

57 So schon *Denninger*, CR 1988, S. 51, 52.

58 *Ferguson*, Emory Law Journal 2012, S. 259, 265.

59 *The Guardian*, vom 21.06.2013, abrufbar unter: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

60 Das entspricht der Datenkapazität von ca. 2.000.000 modernen Smartphones.

61 *The Guardian*, vom 21.06.2013, siehe Fn. 59.

62 *The Guardian*, vom 21.06.2013, siehe Fn. 59.

63 *Washington Post*, vom 06.06.2013, abrufbar unter: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1.