www.jusletter-it.eu

Rolf H. Weber

Big Data: Sprengkörper des Datenschutzrechts?

This article addresses data protection problems arising out of the use of Big Data technologies. In particular risks associated with complex analytical tools which allow for the identification of an individual as well as the loss of control over one's personal data are highlighted. The main focus is thereby placed on developing new concepts to ensure data protection in the context of Big Data analysis.

Category: Scientific Articles
Field of law: Data Protection
Region: Switzerland

Citation: Rolf H. Weber, Big Data: Sprengkörper des Datenschutzrechts?, in: Jusletter IT 11 December 2013

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1 Begriff und Bedeutung von Big Data

1.1 Was ist Big Data?

[Rz 1] Nach einer verbreiteten, technisch ausgerichteten Umschreibung bedeutet Big Data der «Einsatz grosser Datenmengen aus vielfältigen Quellen mit einer hohen Verarbeitungsgeschwindigkeit zur Erzeugung wirtschaftlichen Nutzens».[1] Bezweckt wird mit Big Data die Sammlung und Auswertung umfassender Datenbestände verschiedenster Herkunft in Hochleistungsdatenbanken.[2]

[Rz 2] Bisher hat sich das rechtliche Schrifttum mit Big Data kaum beschäftigt; erst in den letzten Monaten finden sich erste Beiträge zu Big Data, die insbesondere deren Problematik mit Blick auf die Datenschutzgesetzgebung thematisieren. Bezug genommen wird dabei auf schon heute für das Datenschutzrecht schwierige Erscheinungen wie das «Data Warehousing» und das «Data Mining»; Datenschutzrechtler sehen bei Big Data eine Verschmelzung dieser beiden Erscheinungsformen mit den weitreichenden Möglichkeiten des «Cloud Computing».[3]

[Rz 3] Big Data erlaubt insbesondere detaillierte Datenanalysen. Für solche Analysen ist die Art der Daten (z.B. Text, Bild, Video) irrelevant; ebenso kommt es nicht auf die Qualität der Daten an (z.B. strukturierte oder unstrukturierte Daten). Schliesslich spielt die Herkunft der Daten (z.B. unternehmensintern oder extern aus verschiedenen Quellen generiert) keine Rolle; es lassen sich insbesondere auch Daten, die im Internet frei zugänglich sind (z.B. aus sozialen Netzwerken), heranziehen.[4] Die Entwicklung neuer Analyseinstrumente (etwa Hadoop als verteiltes Filesystem mit Prozessoren zur Suche von Daten in einem grossen Datenbestand) unterstützt die praktische Nützlichkeit von Big Data.

---

1 BITKOM Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte, <http://www.bitkom.org/de/publikationen/38337_73446.aspx> (alle Internetquellen wurden zuletzt besucht am 9. Dezember 2013).

2 Christoph Zieger/Nikolas Smirra,Fallstricke bei Big Data-Anwendungen, MMR 2013, 418; Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning?, International Data Privacy Law 2013, Vol. 3, No. 2, 74, 77.

3 Bruno Baeriswyl, «Big Data» ohne Datenschutz-Leitplanken, digma 2013, 14.

4 Zieger/Smirra(Fn. 2), 418; vgl. auch Georg Polzer, Big Data – eine Einführung, digma 2013, 6–9.

[Rz 4] Bereits heute sind die Einsatzzwecke für Big Data-Anwendungen vielfältig: Im geschäftlichen Bereich stehen Analysen mit Blick auf die Einsatzplanung von Personen, die Früherkennung bzw. Fehlerkennung von Markttrends oder die «Competitive Intelligence» im Vordergrund.[5] Anwendungsbereiche im privaten Bereich sind etwa elektronische Gesundheitsdaten oder Kreditinformationen.[6]

1.2 Weshalb ist Big Data datenschutzrelevant?

[Rz 5] Die erhebliche quantitative Veränderung der Datenverarbeitung durch Big Data hat zweifelsfrei auch qualitative Veränderungen zur Folge; mit der Analyse einer viel grösseren Zahl von Daten steigen tendenziell die Datenschutzrisiken, was eine Verbesserung der IT-Sicherheitsinfrastrukturen notwendig macht.[7] Insbesondere hat die durch Big Data neu geschaffene Form der ökonomischen Wertschöpfung mittels Datenauswertung und Datenzugriff im privaten Bereich und im öffentlichen Sektor zur Folge, dass nicht nur die übliche Erstverwendung, sondern verstärkt auch die Zweitverwendung von Daten gewisse Risiken zu verursachen vermag.[8] Nicht übersehen lässt sich aber, dass vorerst noch gesicherte empirische Grundlagen fehlen, welche das Datenschutzrisiko durch Big Data konkret belegen.

[Rz 6] Neue Analysemethoden von Daten setzen voraus, dass die Daten genau gesammelt, aufbewahrt und verwendet werden; je grösser die Anzahl an Datenbeständen ist, umso wahrscheinlicher treten dabei auch mehr «Messfehler» auf, doch erscheint es gleichzeitig als plausibel, dass kleinere «Messfehler» bei viel ausgedehnteren Datenanalysen weniger problematisch sind. Immerhin lässt sich nicht übersehen, dass die Verfügbarkeit von mehr Daten nicht zwingend bedeutet, dass deren Verarbeitung zu mehr Einsicht führt; wie allgemein bei Informationen kann der Umfang des Datenbestands entweder zu Konfusionseffekten (Unklarheiten wegen Prioritäten) oder zu Kassandraeffekten (fehlende Bereitschaft, die Informationen zur Kenntnis zu nehmen) führen.[9]

[Rz 7] Die Datenanalysen durch Big Data stellen zudem einen Schritt weg von der herkömmlichen Kausalitätsdiskussion dar: Im Vordergrund steht bei Vorliegen einer umfassenden Datenverfügbarkeit nicht mehr die Frage nach dem «warum», sondern die Frage nach dem «was».[10] Das Schrifttum spricht deshalb von einer Entwicklung, die von der Kausalitätsdiskussion weg führt zum Konzept der Korrelation.[11]

---

5 Vgl. die vielfältigen Beispiele in BITKOM (Fn. 1); zu den ökonomischen Rahmenbedingungen von Big Data vgl. Guy Chesnot, Cloud computing, Big Data, parallélisme, Hadoop, Paris 2012, 119 ff.; Krish Krishnan, Data Warehousing in the Age of Big Data, Amsterdam et al. 2013, 6 ff., 17 ff.; allgemein auch Rudi Klausnitzer, Das Ende des Zufalls: Wie Big Data uns und unser Leben vorhersehbar macht, Salzburg 2013.

6 Als Beispiele aus Medienberichten vgl. Andreas Hirstein, Die digitale Vermessung der Welt, NZZ am Sonntag vom 30. Juni 2013, 50/51; Michèle Binswanger, Die Diktatur der Daten, Tages Anzeiger vom 6. September 2013, 8; Nicole Beranek Zanon, Heikle Daten, Handelszeitung vom 30. Mai 2013, 63.

7 Andreas Wespi, Big Data: der nächste IT-Sicherheitstrend?, digma 2013, 10-13.

8 Viktor Mayer-Schönberger/Kenneth Cukier, Big Data, A Revolution, New York 2013, 153.

9 Vgl. dazu Rolf H. Weber, Kassandra oder Wissensbroker – Dilemma im «Global Village», in: Becker/Hilty/Stöckli/Würtenberger (Hrsg.), Recht im Wandel seines sozialen und technologischen Umfeldes, Festschrift für Manfred Rehbinder, München 2002, 405–421.

10 Mayer-Schönberger/Cukier(Fn. 8), 12-15.

11 Mayer-Schönberger/Cukier(Fn. 8), 53 und 63.

2 Big Data und Privatheits-Clash

2.1 Datenschutzrechtliches Niemandsland?

[Rz 8] Big Data zeichnet sich dadurch aus, dass eine grosse Datenaggregation stattfindet, die es erlaubt, aus an sich reinen Sachdaten auch Schlüsse auf Personen zu ziehen.[12] Big Data macht Datensammlungen «more granular, more revealing, and more invasive».[13] Die Möglichkeit, aus Sachdaten letztlich ein Personenprofil zu erstellen, führt zu einer Situation, die als «database of ruin» bezeichnet wird.[14]

[Rz 9] Datenschutzgesetze basieren auf dem Konzept der Erfassung von Personendaten. Mit Big Data verursacht indessen auch die Analyse von Sachdaten, die einen Personenbezug zulassen, einen datenschutzrechtlichen Handlungsbedarf. Die Konkretisierung der Anwendung vorhandener Normen ist aber komplex, weshalb zum Teil resigniert festgestellt wird, Big Data liege im «datenschutzrechtlichen Niemandsland».[15]

[Rz 10] Eine zusätzliche Problematik mit Blick auf die Anwendung von Datenschutzgesetzen liegt darin, dass die Technik andere Klassifizierungen verwendet als das Datenschutzrecht mit den Personen- und Sachdaten. In der Technik wird z.B. differenziert zwischen «human-generated data» und «sensor-generated data» (Internet of Things, Geo-Informationen). Eine Parallelisierung der Begrifflichkeit ist kaum möglich.

2.2 Kernschmelze der heutigen Datenschutz-Konzeption?

[Rz 11] Big Data ist regelmässig als strukturierte Datensammlung ausgestaltet, der entsprechende Begriff von Art. 11a DSG ist mithin erfüllt.[16] Ausschlaggebend für die Anwendung des DSG ist somit die Frage, ob die Datenmenge sowie die eingesetzten Datenanalysemethoden zu einer hohen Wahrscheinlichkeit der Identifizierbarkeit einer Person führen.

[Rz 12] Wie erwähnt erfolgt im Kontext von Big Data in der Regel vornehmlich eine Sammlung von Sachdaten. Selbst wenn es sich ursprünglich um Personendaten handelt, sind sie oft anonymisiert, die Problematik besteht aber darin, dass vielfach eine Re-Individualisierung möglich ist. Die Identifizierung einer Person ist überdies umso wahrscheinlicher, je mehr Daten vorhanden sind, d.h. eine sehr grosse Menge zwar anonymisierter Daten lässt gegebenenfalls deren Zuordnung zu einer bestimmten Person zu.[17]

[Rz 13] Studien in den Vereinigten Staaten haben den Nachweis erbracht, dass mit lediglich drei relativ einfachen demographischen Merkmalen, nämlich Geschlecht, Geburtsdatum und fünfstelliger Postleitzahl, zwischen 61% und 87% der amerikanischen Bevölkerung sich eindeutig identifizieren lassen.[18] Überdies haben andere Untersuchungen dargelegt, dass anonyme

---

12 Daniel J. Solove, A Taxonomy of Privacy, Pennsylvania Law Review 154 (2006), 477, 506.

13 Rubinstein(Fn. 2), 77.

14 Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review 57 (2010), 1701.

15 Baeriswyl(Fn. 3), 16.

16 Urs Belser, in: Maurer-Lambrou/Vogt (Hrsg.), Datenschutzgesetz, 2. Aufl. Basel 2006, Art. 11 N 7 ff.

17 Baeriswyl(Fn. 3), 15.

18 Vgl. Günter Karjoth, Sind anonymisierte Daten anonym genug?, digma 2008, 18 ff.

Gen-Sequenzen, die auf öffentlich zugänglichen Forschungs-Datenbanken verfügbar sind, durch Kombination mit wenigen anderen Daten eine «Deanonymisierung» erlauben.[19]

[Rz 14] Die Anwendung des DSG setzt nicht voraus, dass die Bestimmtheit der Person vorliegt, sondern notwendig ist nur die Bestimmbarkeit der Person (Art. 3 lit. a DSG).[20] Reicht deshalb die Menge der vorhandenen Daten aus, um eine Person ohne übermässigen Aufwand zu bestimmen, ist die Datenschutzrelevanz gegeben, weil die mögliche Identifizierung einer Person ein datenschutzrechtlich erfasster Prozess ist.[21]

2.3 Paradoxe in der heutigen Big Data-Diskussion?

[Rz 15] In der Diskussion um die Datenschutzproblematik von Big Data finden sich Hinweise auf das Vorliegen von mindestens drei Paradoxen, die eine kurze Erläuterung verdienen, nämlich (in Anlehnung an Richards und King) das «Transparency Paradox», das «Identity Paradox» und das «Power Paradox»:[22]

[Rz 16] **(i) Transparency Paradox**: Big Data-Analysen bezwecken durch die Sammlung vieler Daten, solche Daten für eine grössere Zahl von Personen transparent und zugänglich zu machen. Die Sammlung der Daten an sich ist indessen unsichtbar und die Instrumente und Techniken sind kaum nachzuvollziehen, insbesondere im Lichte der physischen, technischen und rechtlichen «Layers», auf denen Daten gesammelt werden. Dieser Wiederspruch ist unbefriedigend; zwar mag es Geschäftsgeheimnisse von Unternehmen, die grosse Datensammlungen anlegen, geben, doch wenn gestützt auf solche Datensammlungen auch Entscheide zu Individualpersonen gefällt werden, dann müssten diese Personen wissen, auf welcher Basis es zu solchen Entscheiden gekommen ist.[23]

[Rz 17] In der Lehre wird deshalb für die Einführung eines «Technological Due Process» plädiert, und zwar mit Bezug auf staatliche Stellen wie auf Unternehmen.[24] Die Überwachungsfunktionen in einem komplexen Big Data Analyse-System dürfen nicht geheim sein, insbesondere wenn «decisions are made about individuals by a Kafkaesque system of opaque and unreviewable decision-makers».[25]

[Rz 18] **(ii) Identity Paradox**: Big Data bezweckt, Identifizierungen zu ermöglichen, doch wird dabei die Identität von Individuen gefährdet (sog. informelle Integrität). Insbesondere kann die Souveränität über die eigenen persönlichen Daten einen Schaden nehmen, die sich im Daten-

---

[19] Melissa Gymrek/Amy L. McGuire/David Golan/Eran Halperin/Yaniv Erlich, Identifying Personal Genomes by Surname Inference, Science No. 339/6117, Januar 2013, 321 ff.

[20] Zu den Kriterien vgl. BGE 136 II 508; vgl. nun auch Thomas Probst, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Person im Datenschutzrecht, AJP 2013, 1423 ff.

[21] Baeriswyl(Fn. 3), 15.

[22] Neil M. Richards/Jonathan H.King, Three Paradoxes of Big Data, Stanford Law Review Online 66 (Sept. 3, 2013), 42 ff., <http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data>.

[23] Vgl. dazu Richards/King (Fn. 22), 42–43.

[24] Danielle Keats Citron, Technological Due Process, Washington University Law Review 85 (2008) 1249; vgl. auch Kate Crawford/Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, New York University School of Law, Public Law & Legal Theory Research Paper Series Working Paper No. 13-64, October 2013, 25–26, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784>.

[25] Richards/King (Fn. 22), 43; vgl. auch Neil M. Richards, The Dangers of Surveillance, Harvard Law Review 126 (2013), 1934, 1959-61.

schutzkontext traditionell ausdrückt durch das Recht, allein gelassen zu werden.[26] Letztlich geht es um das Recht einer Person, festzulegen, wer sie sein will.

[Rz 19] Die Gefahr von Big Data besteht somit darin, durch die Identifikation eine Macht über die Offenlegung der Identität zu erreichen, welche Beeinflussungs- und Überzeugungsfunktionen auszuüben vermag.[27] Diese Faktoren können die Kraft und Qualität einer Demokratie beeinträchtigen.

[Rz 20] **(iii) Power Paradox**: Big Data ist ein machtvolles Instrument, das es den Datenanalysten erlaubt, sich ein klareres und schärferes Bild vom Verhalten der Personen, deren Daten gesammelt worden sind, zu machen.[28] Big Data schafft also Gewinner und Verlierer; dabei ist es wahrscheinlich, dass insbesondere die staatlichen Stellen und Unternehmen, welche Big Data-Analysen betreiben, zu den Gewinnern gehören.[29]

[Rz 21] Durch die Schaffung von Privatheit, Transparenz und Personenautonomie sowie durch den Schutz der Identität ist ein gesundes Gleichgewicht zwischen der Macht derjenigen, welche die Daten generieren, und der Stellung derjenigen, die durch Interferenzen und entsprechende Entscheide betroffen sein können, herbeizuführen.[30] Gleichzeitig sind utopische Diskussionen über Big Data herunterzubrechen auf pragmatische Überlegungen zu angemessenen Interessenausgleichen zwischen potentiell widerstreitenden geschäftlichen und privaten Zielvorstellungen.

3 Ansätze für eine zukunftsweisende Datenschutz-Konzeption

3.1 Verzicht auf Differenzierung in Personen- und Sachdaten?

[Rz 22] Wie erwähnt besteht die Problematik von Big Data darin, dass an sich «unproblematische» Sachdaten angesichts der Datenmenge die Identifizierung von Personen ermöglichen, auch wenn die einzelnen Daten keinen direkten Personenbezug aufweisen, oder dass sich anonymisierte Daten re-individualisieren lassen.[31] Entscheidend sind insoweit die angewendeten Analysemethoden, die je nach technologischer Perfektion zur Bestimmbarkeit einer Person führen. Wie ebenfalls schon angesprochen, sind diese Analysemethoden regelmässig nicht ausreichend transparent.[32]

[Rz 23] Gerade im Lichte der Tatsache, dass der Grundsatz der Datenminimierung[33] im Kontext von Big Data nicht spielt, ist mit der heutigen datenschutzrechtlichen Anknüpfung an Personendaten dem beschriebenen technologischen Phänomen der potentiellen Identifizierbarkeit von Personen kaum beizukommen. Ob die Anonymisierung, d.h. der Prozess der Eliminierung von Identifikationsmerkmalen zwecks Schaffung anonymisierter Datenbestände,[34] im Rahmen von

---

[26] Samuel D.Warren/Louis D. Brandeis, The Right to Privacy, Harvard Law Review 4 (1890), 193; Julie E. Cohen, What Privacy Is For, Harvard Law Review 126 (2013), 1904, 1906.

[27] Richards/King (Fn. 22), 44.

[28] Mayer-Schönberger/Cukier(Fn. 8), 11.

[29] Richards/King (Fn. 22), 45.

[30] Richards/King (Fn. 22), 45.

[31] Vgl. vorne Ziff. 1.2.

[32] Vgl. vorne Ziff. 2.3 (i).

[33] Das Bundesgericht spricht von objektiv tatsächlich benötigten Daten (BGE 125 II 473, E. 4).

[34] Dazu Rolf H. Weber/Ulrike I. Heinrich,Anonymization, Berlin 2012, 15 ff.

Big Data die betroffenen Personen vor einem Profiling oder Targeting schützt, erscheint deshalb als zumindest zweifelhaft.[35] Sollen Datenanalysten umfassend dem Datenschutzrecht unterstellt sein, liesse sich dementsprechend erwägen, dessen Anwendungsbereich zu erweitern.

[Rz 24] Die Sammlung von Sachdaten bzw. deren Analyse hätte in einem erweiterten Konzept die datenschutzrechtlichen Prinzipien einzuhalten, wenn die Kombination von Daten einen Personenbezug ermöglicht oder wenn eine Deanonymisierung von Daten den Personenbezug nicht auszuschliessen vermag. Ein solches Konzept wäre aber eine erhebliche Abweichung von allen bisherigen Datenschutz-Konzepten und angesichts des in vielen Ländern tieferen Datenschutzniveaus als in der Schweiz und in der EU nur schwer zu verwirklichen.

3.2 Neue Anforderungen an die Einwilligung durch den Datenherrn?

[Rz 25] Schon heute stellt sich im Online-Verkehr oft die Frage, ob die Einwilligung eines Nutzers/Kunden, dass Daten gesammelt werden dürfen, tatsächlich in ausreichender Weise erfolgt, insbesondere wenn die Erkennbarkeit der Datenbeschaffung (Art. 4 Abs. 4 DSG) den gesetzlichen Anforderungen kaum entspricht; datenschutzrechtlich würde – neben dem Vorliegen überwiegender privater oder öffentlicher Interessen – die Einwilligung an sich eine Datensammlung legitimieren (Art. 13 Abs. 1 DSG).[36] Die anwendbaren Datenschutz-Regulierungen sind auf den Websites der Unternehmen oder der sozialen Netzwerke aber oft nicht ausreichend klar positioniert und dargestellt, was Zweifel an der Unmissverständlichkeit der Einwilligung als berechtigt erscheinen lässt;[37] zudem erweist es sich als zweifelhaft, ob ein reiner Klick ein genügendes Einverständnis darstellt, selbst wenn eine Lektüre der Datenschutz-Regulierungen unterblieben ist.

[Rz 26] Noch problematischer ist die Situation bei Verwendung Allgemeiner Geschäftsbedingungen (AGB), die auch Datenschutz-Regulierungen enthalten. Dass eine solche Einwilligung rechtsgenüglich dem Kriterium der Voraussehbarkeit der Verwendung von Daten entspricht, ist nach verbreiteter Auffassung eher unwahrscheinlich.[38] Der die AGB anklickende Nutzer/Kunde wird in aller Regel kein informiertes Einverständnis geben, was rechtlich betrachtet Zweifel an der AGB-Unterwerfungsbereitschaft aufkommen lässt.

[Rz 27] Angesichts von Sinn und Zweck der Einwilligung ist deshalb zu fordern, dass sie transparent erfolgt und dass der Kunde weiss, welche Datenkategorien und welche Anzahl von Daten den Big Data-Analysen zugeführt werden sollen. Im Zusammenhang mit Big Data muss mithin gefordert werden, dass die Einverständniserklärung des Nutzers/Kunden nur dann als rechtsgültig zu erachten ist, wenn die Einzelheiten der Datenschutz-Regulierungen zur Kenntnis genommen worden sind und wenn keine unerwarteten Datenbearbeitungsmöglichkeiten in versteckter Weise eine Personenidentifizierung erlauben.[39]

---

35 Rubinstein(Fn. 2), 78.

36 Vgl. im Einzelnen dazu Corrado Rampini, in: Maurer-Lambrou/Vogt (Fn. 16), Art. 13 N 3 ff.

37 Vgl. Rolf H. Weber, E-Commerce und Recht, 2. Aufl. Zürich 2010, 456 ff.

38 Weber (Fn. 37), 352; Bruno Baeriswyl,«Soziale Netzwerke» – Taktgeber für die Reform des Datenschutz-rechts, in: Weber/Thouvenin (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich 2012, 93, 100–101.

39 Vgl. auch Baeriswyl(Fn. 3), 16.

3.3 Implementierung eines Accountability-Prinzips?

[Rz 28] «Accountability» (zurückgehend auf das lateinische *accomptare*, d.h. Rechenschaft ablegen)[40] bedeutet, transparent zu machen, wie die Datenbearbeitung und Datenauswertung erfolgen, sowie für die Einhaltung der offen gelegten Grundsätze einzustehen. Wie erwähnt besteht gerade ein Paradox in der heutigen Diskussion zu Big Data darin, dass zwar beliebig viele Daten gesammelt werden, die Analysemethoden indessen geheim bleiben.[41]

[Rz 29] «Accountability» knüpft beim Datenbearbeiter an und will ein Datenschutz-Konzept entwickelt sehen, das konkret vorgibt, dass die Grundsätze der Verhältnismässigkeit, Geeignetheit und Zweckbindung einzuhalten sind.[42] Beim Datenbearbeiter ist das Verständnis dafür zu wecken, dass Datenauswertungen, die einen Persönlichkeitsbezug zulassen, nur unter restriktiven Voraussetzungen als sachgerecht gelten können. Zudem sind die Datensammlungsvorgänge transparent zu machen, was zu einem differenzierten Konzept der Privatheit führen kann.[43]

[Rz 30] «Accountability» lässt sich durch das Aufstellen von verbindlichen Grundsätzen sowie insbesondere durch die Überprüfung der Einhaltung dieser Grundsätze konkretisieren.[44] Als erforderlich erweisen sich deshalb die Einrichtung von Risikoeinschätzungsinstrumenten und der Erlass von Richtlinien zur Data Governance. Sinnvoll ist in diesem Kontext die Erarbeitung und Inkraftsetzung von Verhaltenskodizes sowie die Schaffung von Überwachungsorganen. Denkbar ist auch, dass (private) Zertifizierungsdienste die Datenschutzkonzepte von Big Data-Anbietern prüfen und entsprechende Labels ausstellen.[45]

3.4 Bildung einer Nutzengemeinschaft von Datenverarbeitern und Datenherrn?

[Rz 31] Big Data Analysen bringen Vorteile und Nutzen mit sich, jedenfalls für die Unternehmen, welche die Daten sammeln, oft aber auch für die Individuen. Aus diesem Grunde stellt sich die Frage, ob nicht ein rechtlicher Rahmen geschaffen werden könnte, der dazu führt, dass beide Seiten an diesem Nutzen partizipieren und daraus Vorteile ziehen können (sog. «sharing the wealth strategy»).[46] Unternehmen sollten bereit sein, mit den Individuen den Nutzen zu teilen, der aus der Generierung ihrer Daten entstanden ist.

[Rz 32] Neben der Schaffung ausreichender Transparenz wären insbesondere Zugangsformate einzurichten, welche es den Einzelnen ermöglichen, selber Zugriff auf die Daten zu haben, die Daten gegebenenfalls zu ändern und die Daten auf andere Server zu verschieben (Datenportabilität).[47]

[Rz 33] (a) Als notwendig erweist sich dazu die Schaffung neuer Geschäftsmodelle im Rahmen

---

40 Vgl. Rolf H. Weber, Accountability in the Internet of Things, Computer Law & Security Review 27 (2011), 133, 134.

41 Vgl. vorne Ziff. 2.3 (i).

42 Zum Teil wird in diesem Zusammenhang von Systemdatenschutz oder «Privacy by Design» gesprochen.

43 Vgl. Mayer-Schönberger/Cukier (Fn. 8), 175.

44 Weber (Fn. 40), 135–137.

45 In der Schweiz hat zwar ein von der Schweizerischen Normenvereinigung (SNV) initiiertes Projekt noch keinen praktischen Durchbruch erlebt.

46 Rubinstein (Fn. 2), 81; für Fallstudien vgl. Krishnan(Fn. 5), 101 ff.

47 Rubinstein (Fn. 2), 81.

zu entwickelnder technischer Systeme in Form eines «multi-layered construct»;[48] gleichzeitig geht mit einem solchen Konzept wohl eine Verstärkung des Eigentumsgedankens an den Daten einher.[49] Acht Elemente lassen sich dabei in Betracht ziehen:[50]

[Rz 34] (i) Die Individuen sind das Zentrum der Sammlung von Personendaten, und zwar mit Blick auf deren Verwaltung und deren Gebrauch.

[Rz 35] (ii) Die Offenlegung von Daten hat selektiv zu erfolgen und das Ausmass nicht zu überschreiten, das aus der Sicht des Datenherrn als angebracht erscheint.

[Rz 36] (iii) Kontrollmechanismen hinsichtlich Zweck und Dauer des primären und sekundären Gebrauchs von Daten sind einzuführen; denkbar wäre etwa der Abschluss von «owner data agreements» oder die Einrichtung technischer Vorkehren.

[Rz 37] (iv) Die Datenportabilität ist sicherzustellen, damit der Einzelne über den konkreten Verbleib der Daten bestimmen kann.

[Rz 38] (v) Die Einrichtung eines Identitätsmanagement ist unumgänglich, um zu gewährleisten, dass eine Offenlegung der Identität an nicht berechtigte Dritte vermieden wird.

[Rz 39] (vi) Hohe Sicherheitsvorkehrungen zur Abwehr von illegalen Drittangriffen auf Datenbestände sind zu treffen.

[Rz 40] (vii) Individuen sollen nicht Monopolstrukturen mit Blick auf die Herausgabe von Daten oder dem Abschluss kommerzieller Transaktionen ausgesetzt sein.

[Rz 41] (viii) Durchsetzungsmechanismen sind vorzusehen, um dem Prinzip der «Accountability» tatsächlich Nachachtung zu verschaffen.

[Rz 42] (b) Ein solches Konzept kommt nicht umhin, den Gedanken des «Eigentums» an den Daten, der zu einem besseren Schutz der Privatheit von Informationen beizutragen vermag, zu stärken («propertization»[51]). Bestehen entsprechende Eigentumsrechte, hätten es die Individuen grundsätzlich in der Hand, die Bearbeitung von Daten durch vertragliche Nutzungsbedingungen (z.B. Verwendungsbeschränkungen) zu steuern. Notwendig wäre dafür aber der Abschluss eines individuellen Vertrages, der konkret ausgehandelte Anordnungen zur Art der Nutzung von Daten enthält; zudem dürfte kein Verhandlungsungleichgewicht zwischen den Vertragsparteien bestehen. Aus diesem Grunde ist Vorsicht geboten mit einer vollständigen Überlassung der Datenschutzrealisierung an den Markt, doch lassen sich gewisse Grundregeln durchaus formulieren:[52]

[Rz 43] (i) Gewisse Beschränkungen des Rechts von Individuen, auf ihre Privatheit vollständig zu verzichten, sind gesetzlich vorzusehen (Begrenzungen im Gebrauch von Daten).

[Rz 44] (ii) Regeln sind zu verankern, welche die Unternehmen, die Daten analysieren, verpflichten, Transparenz hinsichtlich der Datensammlungen zu schaffen (Default Rules).

---

48 Nicolas P. Terry, Protecting Patient Privacy in the Age of Big Data, University of MIssouri-Kansas City Law Review 81 (2013), 385, 398.

49 Dazu nachfolgend Ziff. 3.4 (v); ein solcher Ansatz trägt auch dazu bei, den Einzelnen in den Mittelpunkt der Datenschutzdiskussion zu rücken (eingehender dazu Rolf H. Weber, How does Privacy Change in the Age of the Internet?, in: Fuchs/Boersma/Albrechtslund/Sandoval (Hrsg.), Internet and Surveillance: The Challenges of Web 2.0 and Social Media, New York/London 2012, 273, 281 ff.).

50 Eingehender dazu Rubinstein (Fn. 2), 82-83; ähnliche Konzepte finden sich auch bei Terry (Fn. 48), 404 und bei Crawford/Schultz (Fn. 24), 13.

51 Vgl. Paul M. Schwartz, Property, Privacy, and Personal Data, Harvard Law Review 117 (2004), 2055, 2058.

52 Vgl. Schwartz (Fn. 51), 2098–2112; Rubinstein (Fn. 2), 85.

[Rz 45] (iii) Individuen müssen das Recht haben, die Beteiligung an einer Nutzungsgemeinschaft hinsichtlich von Big Data-Analysen zu beenden (Recht auf «Marktaustritt»).

[Rz 46] (iv) Im Falle von Marktmissbräuchen haben Unternehmen, die Big Data-Analysen durchführen, Schadenersatz zu bezahlen (Bestehen einer Haftungsordnung).

[Rz 47] (v) Institutionen sind zu schaffen, welche die Korrektheit der Marktvorgänge überwachen, insbesondere hinsichtlich der Privatheits-Vorgaben der Individuen und der angemessenen Aushandlung von Nutzungsbedingungen (Organisation für die Aufrechterhaltung von Marktmechanismen).

[Rz 48] (c) Schliesslich erweist es sich als unabdingbar, dass personenbezogene Datendienstleistungen zwei technisch ausgerichtete Erfordernisse erfüllen: Einerseits haben Unternehmen, die Big Data-Analysen durchführen, für einen hohen Datensicherheits-Standard einzustehen und andererseits muss der Einzelne in der Lage sein, seine Privatheits-Rechte auch tatsächlich durchzusetzen.[53] Das Eigentums- bzw. Nutzungsrecht lässt sich ebenso durch technische Massnahmen sicherstellen, etwa in der Form des «Digital Rights Management» (DRM) Systems; DRM wird traditionell von Rechteinhabern (bzw. Verwertungsgesellschaften) zur besseren Durchsetzung von Urheberrechten gegenüber unerlaubten Internet-Downloads eingerichtet; denkbar ist der Einsatz eines DRM-Systems aber auch zur Sicherstellung der Privatheit gewisser Informationen.[54]

3.5 Steigende Bedeutung von Verhaltenskodizes?

[Rz 49] Staatliche Datenschutzregulierungen sind regelmässig wenig flexibel; Gesetzgebungsprozesse nehmen zudem oft erheblich Zeit in Anspruch, was dazu führt, dass die rechtlichen Anordnungen im Zeitpunkt des Inkrafttretens technologisch bereits überholt sind.[55] Dieser Regulierungsansatz vermag deshalb den Anliegen der Sachgerechtigkeit und Vorhersehbarkeit der Rechtsanwendung nicht mehr ausreichend Genüge zu tun.

[Rz 50] Verhaltenskodizes sind auch geeignete Instrumente, um über den konkreten Anwendungsbereich der Datenschutzgesetzgebung hinaus Verhaltenserwartungen zu formulieren, die nach verbreiteter Auffassung von den Unternehmen einzuhalten sind; denken lässt sich etwa an ethische Vorgaben.

[Rz 51] Verhaltenskodizes in privaten Unternehmen und in staatlichen Stellen müssen dementsprechend an Bedeutung gewinnen. Zwar haben solche Kodizes die Schwäche, dass sie sich nicht gerichtlich durchsetzen lassen und es zum Teil auch an wirklichen Sanktionen fehlt, doch wirkt oft der moralische Druck der Branche, von den Kodizes nicht abzuweichen.[56] In anderen Bereichen (z.B. Medien, Internet) haben sich Kodizes durchaus bewährt.[57]

---

53 Rubinstein (Fn. 2), 83; zur Intergration von Big Data in Data Warehousing vgl. Krishnan(Fn. 5), 199 ff.

54 Im Einzelnen dazu Jonathan Zittrain, What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, Stanford Law Review 52 (2000), 1201, 2012.

55 Vgl. Rolf H. Weber, Regulatory Models for the Online World, Zürich 2002, 59.

56 Weber(Fn. 55), 84–85.

57 Vgl. Rolf H. Weber/Bianka S. Dörr, Revitalisierung der Selbstregulierung im Medienbereich?, AJP 2002, 213 ff.

3.6 Erweiterte sektorspezifische Regulierungen?

[Rz 52] Sektorspezifische Regulierungen haben gegenüber allgemeinen Normen regelmässig den Nachteil der beschränkten Anwendbarkeit. In gewissen Bereichen und Marktsegmenten ist aber ohne spezifische Regulierungen kaum auszukommen. Im Vordergrund steht das elektronische Gesundheitswesen (E-Health); die weite Verfügbarkeit vieler Daten über einen Patienten ist nicht nur im Interesse der Spitäler und Ärzte, sondern auch im Interesse des Patienten selber, und zwar sowohl im Kontext eines konkreten Krankheitsfalles wie mit Blick auf die Forschung.[58]

[Rz 53] Weitere Bereiche, die mit Sonderregeln zu erfassen wären, betreffen z.B. die immer bedeutender werdenden Transaktion über das Internet of Things[59] und die Kreditinformationen im Finanzbereich.[60]

3.7 Verbesserung der Verfahrensgrundsätze?

[Rz 54] Die Durchsetzung von im Datenschutzgesetz niedergelegten Ansprüchen ist für den Einzelnen oft komplex, zeitintensiv und relativ teuer. Aus diesem Grunde sind Vorkehren zu treffen, um die Rechtsdurchsetzung (z.B. Auskunftsanspruch, Schadenersatz) effizienter zu gestalten; im Vordergrund stehen insbesondere prozessuale Anordnungen, z.B. (i) ausreichende Verfahrensgarantien bei der Rechtsdurchsetzung (Recht auf Gehör, Recht auf gehörige Notifikationen sowie Beweisantretungs- und Zeugenpräsentationsmöglichkeiten, Recht auf Begründung eines Entscheids und Recht auf Anfechtung des Entscheids bei einer höheren Instanz), (ii) die Einrichtung eines Systems der angemessenen Gewaltenteilung, (iii) die Unabhängigkeit von Gerichten und Mediationsstellen sowie (iv) die Implementierung von Regeln, die den Besonderheiten des Verfahrens um Datenoffenlegung angemessen Rechnung tragen.[61]

4 Ausblick

[Rz 55] Big Data ist ein Phänomen, das sich nicht aus der Realität wegdenken lässt; das Phänomen hat in veränderter Form auch schon Vorgänger, wenn man etwa an George Orwell's «Big Brother» denkt. Heute ist Big Data vornehmlich eine US-Erscheinung; je nach gesellschaftlicher Philosophie bedeutet Verfügbarkeit von Daten aber nicht, dass ein Zugriff auf diese Daten immer auch gerechtfertigt ist.

[Rz 56] Ganz abgesehen von der Problematik grenzüberschreitender Datenlieferungen[62] sind die heutigen Datenschutzgesetze nicht ausreichend für die neuen Herausforderungen und Risiken von Big Data gewappnet. Diese Einsicht bedeutet aber nicht, dass nun hektisch vorzunehmende Datenschutz-Gesetzanpassungen erforderlich sind. Vielmehr wäre es angebracht, grundsätzlich darüber nachzudenken, welche Ziele berechtigte Anliegen wie Persönlichkeitsschutz und infor-

58 Eingehend dazu Terry (Fn. 48), 395 ff., 401 ff., 405 ff.; Crawford/Schultz (Fn. 24), 6, 9.

59 Vgl. Rolf H. Weber/Romana Weber, Internet of Things – Legal Perspectives, Zurich 2010, 47 ff.

60 Vgl. Rolf H. Weber, E-Governance in der Finanzdienstleistungsbranche, in: Strebel-Aerni (Hrsg.), Finanzmärkte im Banne von Big Data, Zürich 2012, 159, 170.

61 Eingehender dazu Crawford/Schultz (Fn. 24), 14 ff., 19 ff., 24 ff.

62 Vgl. Rolf H. Weber, Transborder data transfers: concepts, regulatory approaches and new legislative initiatives in: International Data Privacy Law, February 2013, 1–14.

mationelle Selbstbestimmung anzustreben beabsichtigen.

[Rz 57] Mit einer solchen Optik treten neue Elemente in den Vordergrund, etwa die Sicherstellung der Kompatibilität von Datenverarbeitungen mit der ursprünglichen Zweckbestimmung, die Ausrichtung datenschutzrechtlicher Normen auf eine sachgerechte Risikoorientierung (organisatorische und technische Massnahmen), die Schaffung einer angemessenen Data-Governance-Kultur sowie die Implementierung von Rechenschafts- und Verantwortungsprinzipien («Accountability»). Solche Konzepte gehen über die traditionellen Datenschutzgesetze hinaus und verlangen sowohl eine breite, zivilgesellschaftliche Diskussion über die Legitimität von Datenbearbeitungen als auch eine intellektuelle Offenheit für ein neues weit verstandenes Datenrecht.

Prof. Dr. iur. Rolf H. Weber ist Ordinarius für Privat-, Wirtschafts- und Europarecht an der Universität Zürich, Visiting Professor an der Hong Kong University und praktizierender Rechtsanwalt in Zürich.