www.jusletter-it.eu

René Huber

«Big Data», das kantonale Recht und der Datenschutz

Today all the information about us ends up as digital data. The amount of data increases rapidly. Big Data tools provide strong instruments to analyze these data in order to gain new information and knowledge. Big Data is not only an issue for companies — but also for the public administration. The administration has countless databases containing data about citizens and firms. Is the public administration of the Cantons allowed to join the party? If so, what is the legal framework? And what are the implications of data protection? This report gives a short overview of the privacy aspects in the field of Big Data within the cantonal legal framework.

Category: Articles
Field of law: Big Data, Open Data & Open Government; Data Protection
Region: Switzerland

Citation: René Huber, «Big Data», das kantonale Recht und der Datenschutz, in: Jusletter IT 21 May 2015

Inhaltsübersicht

1 Einleitung

[Rz 1] Es ist offensichtlich — wir leben im Informationszeitalter. Durch die Digitalisierung aller Lebensbereiche fallen immer mehr Daten an.

[Rz 2] Hier soll stellvertretend nur auf unsere Kommunikationsgeräte, auf Internet und Social Media oder das «Internet der Dinge» und den zunehmenden Einsatz von Sensoren in Alltagsgegenständen hingewiesen werden. Alle unsere Äusserungen, überhaupt alles über uns liegt digital — in Datenbeständen abgelegt — vor. Der Datenbestand wächst exponentiell. Dieser Fundus an Daten kann für Wirtschaft und Staat höchst wertvoll sein. Nicht zu Unrecht werden die Da-

tenbestände denn auch als «das Öl des 21. Jahrhunderts» bezeichnet.[1] Durch den technischen Fortschritt der letzten Jahre in den Bereichen Hardware/Software sowie der Übertragungstechnik ist es nun möglich, diese «Ölvorkommen» auch zu fördern, somit praktisch unbeschränkt grosse Datenbestände effizient und effektiv zu analysieren und auszuwerten.

[Rz 3] Was die Technik hier ermöglicht, muss aber in einem gesellschaftlichen Zusammenhang gesehen werden, haben doch Speicherung und Analyse einer Vielzahl von Daten über Personen durch Wirtschaft und Staat in aller Regel[2] grosse Auswirkungen auf jede einzelne betroffene Person.[3] Angesprochen und gefordert ist daher das Recht, insbesondere die Regelung des Schutzes der Privatsphäre.

[Rz 4] Big Data ist nicht nur ein Thema der Wirtschaft. Auch der Staat verfügt über Schätze, die allenfalls gehoben werden wollen. Es ist offensichtlich — hier ist mit massiven Konflikten bezüglich des Datenschutzrechts zu rechnen. Es lohnt sich deshalb, einen Blick auf die Rechtslage von Big Data im öffentlichen Recht zu werfen. Da in der Schweiz den Kantonen bekanntlich in vielen Bereichen eine abschliessende Kompetenz zur Gesetzgebung zukommt, soll im Folgenden im Sinne einer Auslegeordnung geprüft werden, wie es um die Rechtslage von Big Data im öffentlichen Recht der Kantone im Hinblick auf den Datenschutz steht. Da es sich um einen Überblick in grundsätzlicher Hinsicht handelt, wird punktuell auf die Rechtslage verschiedener Kantone Bezug genommen.

2 Big Data — was ist das?

[Rz 5] Weder eine verbindliche noch eine exakte Definition von Big Data liegt vor.[4] Im Zusammenhang mit Big Data werden üblicherweise jedoch die folgenden vier[5] Aspekte[6] bei der Auswertung und Analyse von Daten als zentral betrachtet[7]:

- *Datenmenge*: Die zu analysierenden Datenbestände können letztlich beliebig gross sein (die Auswertungstools sind in der Lage, die Datenbearbeitung auf eine Vielzahl von Rechnern zu verteilen).
- *Verarbeitungsgeschwindigkeit*: Diese ist in aller Regel sehr hoch (Resultate von Auswertungen können — wie etwa bei einer Google-Suche — innerhalb von Sekunden vorliegen).
- *Datenheterogenität* (auch: Datenvielfalt): Daten müssen nicht wie bis anhin in einem bestimmten Datenformat und strukturiert in einer Datenbank abgelegt sein, um auswertbar zu sein.

---

1 Andreas Wespi, Big Data: Technische Aspekte, S. 15 f. (in Big Data und Datenschutz — Gegenseitige Herausforderungen, Rolf H. Weber/Florent Thouvenin [Hrsg.], Zürich 2014).

2 Ausser es fallen Auswertungen ohne jeglichen Personenbezug an (Statistik, technische Forschungsresultate etc.). Vgl. dazu Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, S. 45 (im Folgenden: WP 29/203/S.).

3 WP 29/203/S. 35, S. 45 ff. (zit. in FN 2).

4 Ebenso etwa Niko Härting, Profiling: Vorschläge für eine intelligente Regulierung, Computer und Recht, 2014/8 S. 528—536, S. 528 f.

5 Teilweise werden auch nur die ersten drei «V» genannt (so etwa: Jean-Pierre König, Suchmaschinen und Social Media, S. 31 f. [in Weber/Thouvenin, zit. in FN 1]).

6 Auch als die vier «V» bezeichnet: Volume (Menge), Velocity (Geschwindigkeit), Variety (Vielfalt) und Veracity (Richtigkeit). Weitere Fundstellen bei Florent Thouvenin, Grundprinzipien des Datenschutzrechts auf dem Prüfstand, S. 62/FN 1 (in Weber/Thouvenin, zit. in FN 1).

7 Vgl. etwa: Thomas Hoeren (Herausgeber), Big Data und Recht, München 2014 (im Folgenden: Hoeren, Big Data, S.), S. 4; Wespi, Big Data: Technische Aspekte, S. 4 f. (in Weber/Thouvenin, zit. in FN 1).

Vielmehr darf es sich um beliebige Formate an beliebigen Orten handeln (somit etwa: Tabellen, Text, Bilder, Sensor-, Audio- oder Videodateien).
- *Datenqualität* (auch: Datenrichtigkeit): Die Datenbestände können auch «unscharfe», «ungenaue», ungesicherte oder ungeprüfte Daten enthalten (dies kann durch entsprechende Analysetools berücksichtigt und aufgefangen werden).

3 Abgrenzungen

3.1 Beschränkung auf datenschutzrechtliche Aspekte

[Rz 6] Im Folgenden wollen wir uns auf die datenschutzrechtlichen Aspekte von Big Data in der kantonalen[8] Verwaltung beschränken. Nicht eingegangen wird etwa auf Fragen des Urheber-, des Straf-, des Haftungs- oder des Archivrechts.[9]

[Rz 7] Im Bereich von Big Data stellt sich oft auch die Frage, ob die damit im Zusammenhang stehenden Datenverarbeitungen in jeder Beziehung sicher vorgenommen werden — das Thema IT-Security ist angesprochen. Allfällige Datenverarbeitungen im Rahmen von Big Data durch die Kantone haben sich an die allgemeinen kantonalen gesetzlichen Vorgaben bezüglich der Informationssicherheit zu halten. Es ist darauf zu verweisen. Auf Ausführungen bezüglich IT-Security kann hier deshalb verzichtet werden.

3.2 Nicht im Fokus: Forschung, Planung, Wissenschaft und Statistik

[Rz 8] Die kantonalen Datenschutzrechte sehen für die Zwecke Forschung, Planung, Wissenschaft und Statistik in der Regel besondere Vorschriften vor,[10] welche diese Datenbearbeitungen privilegieren. Quelldaten sind zwar meist Personendaten und die Ergebnisse enthalten allenfalls auch noch Angaben zu bestimmten oder bestimmbaren Personen — jedoch erfolgen diese Bearbeitungen zu *nicht personenbezogenen Zwecken*. Rechtliche Vorgabe ist denn auch, dass jeglicher Personenbezug sobald als möglich, jedenfalls spätestens bei der Publikation, unwiderruflich entfernt wird.

[Rz 9] Unter Beachtung der entsprechenden kantonalen Vorgaben des Datenschutz- bzw. Statistikrechts ist der Einsatz von Big Data Tools im Rahmen von Forschung, Planung, Wissenschaft und Statistik grundsätzlich *zulässig*.

4 Zum Datenbestand in der kantonalen Verwaltung

[Rz 10] Die kantonale öffentliche Verwaltung verfügt über umfassende Datenbestände aus den verschiedensten Lebensbereichen der Einwohnerinnen und Einwohner sowie weiterer Personen[11].

---

8 Grundsätzlich analog ist die Rechtslage für *kommunale Behörden*.

9 Vgl. zu den von Big Data allenfalls tangierten Rechtsgebieten Hoeren, Big Data, IX-XIV(zit. in FN 7).

10 Vgl. etwa: §4 Bst. e DSG-ZG (BGS 157.1), §10 IDG-BS (SG 153.260), §19 IDAG-AG (SAR 150.700), Art. 12 DSG-SH (SHR 174.100), Art. 15 LPDP-TI (RL 1.6.1.1), Art. 24 LPrD-VD (RSV 172.65).

11 Etwa: Unternehmen, die Vertragspartner des Kantons sind; Straftäter, die Wohnsitz in einem anderen Kanton oder im Ausland haben etc.

In aller Regel haben die Daten der Verwaltung eine sehr hohe Qualität, was für Auswertungen wertvoll ist.

[Rz 11] Einige kantonale Datenschutzstellen veröffentlichen im Internet ein Verzeichnis aller im jeweiligen Kanton geführten Datensammlungen (als «Register der Datensammlungen» bezeichnet). Dabei weisen die folgenden Kantone die folgende Anzahl unterschiedlicher Datensammlungen nach: Kanton Nidwalden ca. 115[12], Kanton Obwalden ca. 170[13], Kanton Schwyz ca. 170[14], Kanton Zug ca. 350[15], Kanton St. Gallen rund 700[16]. Obwohl alle aufgeführten Kantone in etwa die gleichen Aufgaben zu erfüllen haben, somit ungefähr dieselbe Anzahl Datensammlungen aufweisen sollten, sind hier offensichtlich ganz erhebliche Unterschiede festzustellen. Diese lassen sich damit erklären, dass in den einen Kantonen verschiedene Datenbestände in einer einzigen Datensammlung zusammengefasst, in anderen Kantonen hingegen als separate Datensammlungen registriert werden.

5 Mögliche Einsatzgebiete von Big Data in den Kantonen

[Rz 12] Big Data ist nicht nur ein Thema, das die Wirtschaft interessiert — vielmehr kann diese Art der Datenbearbeitung zukünftig auch für kantonale Behörden eine Rolle spielen. Im Folgenden werden ein paar naheliegende mögliche Anwendungsbeispiele aufgeführt. Beim Einsatz von Big Data setzt aber nur die Phantasie die Grenzen, wird doch auf diesem Gebiet in Zukunft schlechterdings «alles» möglich sein.

5.1 Polizei/Strafverfolgung/Staatssicherheit

[Rz 13] Richter[17] zitiert in seinen Ausführungen einen hohen deutschen Polizeibeamten, demgemäss Big Data offenbar wie folgt zum Einsatz kommen kann: Werden in einem bestimmten Wohn- oder Industriegebiet, das für Einbrecher interessant sein könnte, auffällig viele Smartphones mit ausländischen Telefonnummern und gleichzeitig unüblich viele Transportfahrzeuge mit ausländischer Immatrikulation erkannt,[18] rückt die Polizei zu einem Augenschein vor Ort aus. Es wird hier somit versucht, aufgrund von Big Data zukünftiges Handeln vorherzusehen[19] — «Predictive Policing» ist hier das Stichwort.[20]

---

12 Abschnitt «Register der Datensammlungen» unter «www.kdsb.ch».

13 Abschnitt «Register der Datensammlungen» unter «www.kdsb.ch».

14 Abschnitt «Register der Datensammlungen» unter «www.kdsb.ch».

15 Vgl. Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Zug 2014, S. 23 sowie das via Website zugängliche Online-Register.

16 Das Register ist auf der Website der Fachstelle für Datenschutz des Kantons St. Gallen zugänglich.

17 Frederick Richter, Aus Sicht der Stiftung Datenschutz — Privacy in the age of Big Data, Privacy in Germany/PinG 2014/05 S. 203—205, S. 204.

18 Nicht ausgeführt wird, ob diese Daten vom System der LKW-Maut/Toll Collect, aus automatisierten Auswertungen von Videoüberwachungen oder auf einem anderen Weg erhoben werden.

19 Vgl. zu Strafverfolgung, Gefahrenabwehr und Gefahrenprognose: Thilo Weichert, Big Data und Datenschutz — Chancen und Risiken einer neuen Form der Datenanalyse, Zeitschrift für Datenschutz/ZD 2013 S. 251—259, S. 253 mit weiteren Hinweisen in FN 26.

20 Vgl. dazu etwa die Antwort der Bundesregierung vom 3. März 2014 / Drucksache 18/707 auf die Kleine Anfrage «Computergestütztes Aufspüren von unerwünschtem Verhalten im öffentlichen Raum» vom 13. Februar 2014 / Drucksache 18/540.

[Rz 14] Im Jahr 2014 berichteten die Medien über eine Demonstration in Kiew.[21] Dabei habe die Polizei Demonstrierende eingekesselt und offenbar auf elektronischem Weg deren[22] Handydaten erfasst, um ihnen anschliessend per SMS mitzuteilen, dass sie nun als Teilnehmer einer gewalttätigen Demonstration registriert seien. Die ukrainischen Telekom-Unternehmen bestritten in der Folge, der Polizei Nutzerdaten geliefert zu haben.[23]

[Rz 15] Aufnahmen von Datenbrillen[24] oder Videoüberwachungsanlagen des öffentlichen Raums können mit Gesichtserkennung-Software analysiert und mit weiteren vorhandenen bzw. von Dritten beschafften Daten verknüpft werden.

5.2 Energieversorgung

[Rz 16] Die Versorgung der Bevölkerung mit Strom, Gas oder Fernwärme ist eine öffentliche Aufgabe. Für die Erfassung des Energiebezugs kommt je länger je mehr «Smart Metering» zum Einsatz. Weil die Erfassungsgeräte Verbrauchsdaten kontinuierlich erfassen können, wird ein sehr aussagekräftiges Profil über das Verhalten der Haus- oder Wohnungsbewohnenden angelegt. Auch hier besteht die Möglichkeit, die Verbrauchsdaten mit Personendaten aus anderen Bereichen zu verknüpfen.[25]

5.3 Gesundheit

[Rz 17] Die meisten Kantone betreiben selber Spitäler oder lassen solche in mehr oder weniger selbständiger Form führen. Bei den Krankenhäusern fallen aus den verschiedensten Bereichen grosse Mengen an Gesundheitsdaten an. Zu denken ist etwa an Krankenberichte, Laboruntersuchungen, MRI/CT/Röntgen, Forschung, Administration etc. Diese Datenbestände — insbesondere in Kombination mit Daten aus anderen Bereichen — können mit Instrumenten von Big Data analysiert bzw. erschlossen werden.

5.4 Personelles/Human Ressources

[Rz 18] Die Mitarbeitenden der Verwaltung können durch die Analyse ihrer verschiedenen elektronischen Arbeitsgeräte — PC/Notebook, Festtelefon, Handy oder Pager — bezüglich Arbeits-

---

21 The Guardian, Text messages warn Ukraine protesters they are «participants in mass riot», 21. Januar 2014; Zeit Online, Ukrainische Polizei verhaftet angebliche Protestführer, 21. Januar 2014.

22 Da die Geolokalisation nicht mit absoluter Genauigkeit vorgenommen werden kann, sind dabei auch Personen erfasst worden, die zwar nicht an der fraglichen Demonstration teilgenommen, sich jedoch in der Nähe aufgehalten haben.

23 Es ist denkbar, dass die Polizei zur Erfassung der in der Funkzelle in Betrieb stehender Handys einen «IMSI-Catcher» (Gerät, das ein Mobilfunknetzwerk bzw. eine Basisstation simuliert) eingesetzt hat.

24 Etwa «Google Glass» (Google hat Anfang 2015 zwar den Verkauf eingestellt, jedoch vermeldet, an der Weiterentwicklung solcher Geräte zu arbeiten), «SmartEyeglass» von Sony oder ähnliche Geräte.

25 Dies gilt jedenfalls dann nicht, wenn die gesetzliche Regelung eine Datenweitergabe ausdrücklich verbietet, wie dies in §4a des Energiegesetzes des Kantons Zug (BGS 740.1) der Fall sein wird, wenn die entsprechende Teilrevision bezüglich der Regelung des «Smart Meterings» in Kraft tritt (der Zuger Kantonsrat hat diese Teilrevision am 2. April 2015 in zweiter Lesung beschlossen, dass dagegen das Referendum ergriffen wird, ist nicht zu erwarten. Dem Inkrafttreten im Juli 2015 dürfte nichts im Wege stehen.).

weise, Effizienz, Verhalten und Compliance systematisch, exakt und permanent automatisiert überwacht werden.

[Rz 19] Big Data Auswertungen können aber auch bei der Rekrutierung von neuen oder bei der Evaluation von bisherigen Mitarbeitenden eingesetzt werden.

5.5 Kontrolle und Überwachung

[Rz 20] Der Staat ist in vielen Bereichen auf Angaben der Bürgerinnen und Bürger angewiesen (etwa: Steuern, Soziales, Wohnsitz). Dabei muss sich der Staat oft ungeprüft darauf verlassen, dass die ihm gemachten Angaben korrekt sind. Big Data kann mächtige Instrumente zur automatisierten Kontrolle und Überwachung der unterschiedlichsten Lebenssachverhalte zur Verfügung stellen: Erscheinen die Angaben des Steuerpflichtigen insgesamt als korrekt oder meldet Big Data, dass sie durch einen Mitarbeitenden näher zu überprüfen sind?

5.6 Gewährleistung der IT-Sicherheit

[Rz 21] Die meisten Kantone verfügen über zentrale verwaltungseigene Informatikdienstleister. Bei diesen können zur Gewährleistung der IT-Security ein- und ausgehende Datenströme mittels Big Data Tools analysiert werden.[26]

6 Zur Rechtslage — eine Auslegeordnung

[Rz 22] Im gesamten Werk «Big Data und Recht» von Hoeren[27] finden sich bezüglich Big Data in der Verwaltung mit dem Hinweis auf Weichert[28] nur die beiden folgenden Sätze: «Öffentliche Stellen verarbeiten Daten grundsätzlich aufgabenbezogen und unterliegen dabei einem strengen Zweckbindungsgrundsatz. Insoweit kommt eine Big-Data-Auswertung durch öffentliche Stellen nur aufgrund gesetzlicher Spezialregelungen in Betracht.» Können wir das Thema Big Data im staatlichen Umfeld damit zur Seite legen? M.E. lohnt es sich, eine kleine Auslegeordnung der datenschutzrechtlichen Aspekte vorzunehmen.

6.1 Vorweg: Personendaten, Sachdaten — und anonymisierte Daten?

6.1.1 Personendaten

[Rz 23] Das Datenschutzrecht schützt die Persönlichkeit bzw. die Privatsphäre von *Personen*. Es ist somit nur dann anwendbar, wenn Daten bearbeitet werden, die einen Bezug zu einer natürlichen oder juristischen Person haben. Die Person muss bestimmt oder bestimmbar sein. Diese Regelung

[26] Weitere Hinweise dazu bei Florent Thouvenin, Grundprinzipien des Datenschutzrechts auf dem Prüfstand, S. 62/FN 4 (in Weber/Thouvenin, zit. in FN 1).

[27] Hoeren, Big Data, S. 78 (zit. in FN 7).

[28] Thilo Weichert, Big Data und Datenschutz — Chancen und Risiken einer neuen Form der Datenanalyse, Zeitschrift für Datenschutz/ZD 2013 S. 251—259.

finden wir nicht nur im Bundesrecht,[29] sondern ebenso in allen kantonalen Datenschutzregelungen.[30]

[Rz 24] *Bestimmt* ist eine Person, wenn sich aus der Information selber bzw. aus dem direkten Zusammenhang ergibt, um welche Person es sich handelt.[31] Zu denken ist etwa an Informationen, die einem Personalausweis entnommen werden können[32] oder solchen aus ausgefüllten Formularen, wie etwa der Steuererklärung, einem Baugesuch oder einer Strafanzeige. In allen diesen Fällen ist direkt ersichtlich, auf welche Person sich die fraglichen Informationen bzw. Datenbearbeitungen beziehen.

[Rz 25] *Bestimmbar* ist eine Person, wenn die Möglichkeit besteht, anhand von Abklärungen oder in Kombination mit anderen Daten ihre Identität festzustellen. Beispielsweise kann anhand der Adresse einer Liegenschaft ohne weiteres deren Eigentümer[33] oder anhand des Autokennzeichens der Fahrzeughalter[34] ermittelt werden.

6.1.2 Sachdaten

[Rz 26] Liegen Daten vor, die keinerlei Zusammenhang zu einer Person haben, handelt es sich um *Sachdaten*. Zu denken ist etwa an Statistiken, Strategien, Resultate von Schadstoffmessungen des Seewassers oder meteorologische Daten. Die Unterscheidung zwischen Personendaten und Sachdaten ist von grosser praktischer Bedeutung, da die Bearbeitung von Sachdaten nicht dem Datenschutzrecht[35] unterliegt. Im Zusammenhang mit Big Data ist zudem zu beachten, dass die kantonalen Datenschutzgesetze nur diese beiden Kategorien kennen — tertium non datur. Eine dritte Kategorie oder Zwischentöne gibt es somit im geltenden Recht nicht. Darauf wird zurückzukommen sein.[36]

6.1.3 Anonymisierte Daten

[Rz 27] Bei *anonymisierten Daten* handelt es sich um Daten, die ursprünglich einen Personenbezug aufwiesen, jedoch derart bearbeitet wurden, dass dieser Bezug zu einer bestimmten oder be-

---

29 Vgl. Art. 3 Bst. a DSG (SR 235.1): «Personendaten (Daten): alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen».

30 §3 IDG-ZH (LS 170.4), Personendaten: «Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen.» Vgl. dazu Beat Rudin, N 15 ff. zu §3, Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich.Gemäss §2 Bst. a DSG-ZG (BGS 157.1): «Personendaten (im Folgenden «Daten») sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person oder auf eine Personengesellschaft des Handelsrechts beziehen.»Vgl. Art. 4 Bst. a LIPAD-GE (RS A 2 08): «données personnelles (ou données), toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable». Gemäss dem Datenschutzrecht des Kantons Tessin muss ein direkter oder *indirekter* Bezug zu einer Person bestehen (Art. 4 Abs. 1 LPDP-TI [RL 1.6.1.1]): «Sono considerati dati personali le indicazioni o informazioni che direttamente o indirettamente permettono di identificare una persona, sia essa fisica o giuridica».

31 Vgl. Gabor P. Blechta, N 7 ff. zu Art. 3, Basler Kommentar Datenschutzgesetz, Urs Maurer-Lambrou/Gabor P. Blechta (Hrsg.), 3. Aufl., Basel 2014 (im Folgenden: BSK DSG).

32 Vgl. Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II 413, S. 444.

33 Aufgrund einer Anfrage beim Grundbuchamt gestützt auf Art. 970 Abs. 2 Ziff. 2 ZGB (SR 210).

34 Gestützt auf Art. 126 Verkehrszulassungsverordnung (SR 741.51).

35 Zu beachten ist, dass bei der Verwaltung vorhandene Sachdaten allenfalls dem Amtsgeheimnis (bzw. einem Spezialgeheimnis) unterliegen können.

36 Vgl. hinten Abschnitt 9.

stimmbaren Person nicht mehr besteht.[37] Es wird somit das Band zu einer Person durchgeschnitten. Wichtig ist dabei, dass dieser Anonymisierungsprozess vollständig, umfassend und irreversibel vorgenommen wird.[38] Wie im Bundesrecht[39] sehen übrigens die meisten älteren kantonalen Datenschutzgesetze ausdrücklich vor, dass die Anonymisierung eine gleichwertige[40] Alternative zur Löschung von Personendaten darstellt.[41] Neuere kantonale Gesetze hingegen sehen am Ende des Lebenszyklus zu Recht nur noch die Alternativen Archivierung oder Vernichtung vor.[42]

[Rz 28] Es stellt sich die Frage, wann Personendaten rechtsgenügend anonymisiert sind, damit die Zuordnung zu einer Person aufgrund der Restdaten nicht mehr möglich ist, somit «jeder Bezug zur betroffenen Person ausgeschlossen ist».[43] Zuzustimmen ist Rosenthal, der fordert, dass für *niemanden*, somit auch für den Datenbearbeiter selber nicht mehr bekannt ist, zu welcher Person die Daten vor der Anonymisierung einen Bezug hatten.[44] Gemäss Jöhri darf selbst auch der Einsatz von «ausserordentlichem Aufwand» nicht zur Identifikation der betroffenen Person führen.[45,46]

[Rz 29] Die Lehre geht mit dem Bundesgericht[47] davon aus, dass jeweils der *konkrete Einzelfall* zu prüfen ist.[48] Entscheidend ist dabei einerseits, welcher Aufwand betrieben werden muss, um eine Information einer Person zuordnen zu können (objektive Komponente) und andererseits, welches Interesse der Datenbearbeiter an der Identifizierung hat, somit bereit ist, den erforderlichen Aufwand auch zu betreiben (subjektive Komponente).[49] Beim Ganzen spielt auch der Stand der Technik eine wichtige Rolle.[50]

---

37 Vgl. Robert Bühler, N 16 ff. zu Art. 21, BSK DSG (zit. in FN 31).

38 Vgl. dazu Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, S. 3 ff. (im Folgenden WP 29 05/2014).

39 Art. 21 Abs. 2 Bst. a DSG.

40 Gleiche Rechtslage im Bundesrecht, vgl. Rober Bühler, N 22 zu Art. 21, BSK DSG (zit. in FN 31).

41 Vgl. §11 DSG-ZG (BGS 157.1): «Organe müssen Daten, die sie nicht mehr benötigen, anonymisieren oder vernichten, soweit die Daten nicht unmittelbaren Beweiszwecken dienen oder dem zuständigen Archiv abzuliefern sind.» Ähnlich Art. 12 Abs. 2 Bst. a DSG-GL (GS I F/1) bzw. Art. 21 Abs. 5 Bst. a LPDP-TI (RL 1.6.1.1).

42 Vgl. §21 Abs. 1 IDAG-AG (https://gesetzessammlungen.ag.ch/frontend/versions/1745SAR 150.700), Art. 52 CPDT-JU/NE (RSN 150.30) sowie §5 Abs. 3 IDG-ZH (LS 170.4) (dazu Bruno Baeriswyl, N 18 zu §5, Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich). Zu BS vgl. Beat Rudin, N 17 zu §16, Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt.

43 Vgl. 11. Tätigkeitsbericht 2003/2004 des Eidg. Datenschutzbeauftragten, S. 39; Robert Bühler, N 16 ff. zu Art. 21, BSK DSG (zit. in FN 31).

44 David Rosenthal, N 35 zu Art. 3, Handkommentar zum Datenschutzgesetz, Zürich 2008.

45 Yvonne Jöhri, N 28 zu Art. 21, Handkommentar zum Datenschutzgesetz, Zürich 2008.

46 Weniger streng ist diesbezüglich das deutsche Datenschutzrecht, das in §3 Abs. 6 des deutschen Bundesdatenschutzgesetzes (BDSG) die Anonymisierung wie folgt definiert: «Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäSSig grossen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.»

47 BGE 136 II 508 E. 3 S. 513 in Sachen Logistep AG («Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor [BBI 1988 II 413, S. 444 f. Ziff. 221.1]. Die Frage ist abhängig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge.» In casu: Bejahung des Personenbezugs von IP-Adressen.).

48 Robert Bühler, N 17 ff. zu Art. 21, BSK DSG (zit. in FN 31); grundlegend: Thomas Probst, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Person im Datenschutzrecht, AJP 2013 S. 1423—1436, S. 1431 (mit weiteren Literaturangaben); Bruno Baeriswyl, «Big Data» ohne Datenschutz-Leitplanken, digma 2013/1 S. 15.

49 BGE 136 II 508 E. 3.2 S. 514; David Rosenthal, «Logistep»: Offenbar ein Einzelfallentscheid, digma 2011/1 S. 41.

50 BGE 136 II 508 S. 514; Gabor P. Blechta, N 13 zu Art. 3, BSK DSG (zit. in FN 31); David Rosenthal, «Logistep»:

[Rz 30] Schon immer war die Frage entscheidend, was vorzukehren ist, damit aus Personendaten rechtsgenügend anonymisierte Daten — somit Sachdaten — werden. Aufgrund von Big Data hat sie jedoch eine neue Dimension erhalten, ist doch nun die Verknüpfung von beliebigen Daten, Informationen und Formaten in einer solchen Weise möglich, dass oft wieder ein Personenbezug hergestellt werden kann.[51]

[Rz 31] So zeigte eine oft zitierte Studie aus den USA auf, dass offenbar 87% der gesamten Bevölkerung der Vereinigten Staaten — somit 216 von 248 Millionen Personen — anhand der drei folgenden Kriterien identifizierbar sind: Geburtsdatum, Postleitzahl des Wohnorts und Geschlecht.[52] Eine Untersuchung aus dem Jahr 2006 kam hingegen zum Schluss, dass nicht 87%, sondern nur gut 63% der US-Bevölkerung aufgrund dieser drei Kriterien identifizierbar sei.[53] Unabhängig davon, ob 63% oder 87% zutreffend sind, erstaunt doch sehr, dass jedenfalls mehr als die Hälfte der US-Bevölkerung anhand von bloss drei Kriterien identifizierbar ist. Werden somit Resultate medizinischer Studien veröffentlicht, welche diese Informationen noch enthalten — was in den USA offenbar häufig geschieht — , ist es ohne weiteres möglich, den Namen des betroffenen Patienten zu ermitteln und dadurch Zugang zu seinen Gesundheitsdaten zu erlangen.

[Rz 32] Es stellt sich nun die Frage, ob die Verknüpfung von (vielen) anonymisierten Daten grundsätzlich (stets) eine Re-Individualisierung ermöglicht oder ob die (vermeintlich) anonymisierten Daten eben bloss nicht effektiv genug anonymisiert wurden. Würde im vorstehenden Beispiel etwa nicht das Geburtsdatum, sondern nur das Geburtsjahr — oder noch besser, Altersklassen (z.B. aggregiert aus fünf Jahrgängen) — veröffentlicht und zudem nicht die Postleitzahl, sondern bloss Angaben zum County — oder gar nur zum US-Gliedstaat — so könnte hier (wohl) *kein* Personenbezug mehr hergestellt werden.

[Rz 33] Eine Re-Individualisierung kann demnach (wohl) in den meisten Fällen verhindert werden, wenn nur die Vorgaben bezüglich rechtsgenügender Anonymisierung streng genug sind. Es ist jedoch davon auszugehen, dass dies nur in der Theorie funktioniert, nicht aber in der Praxis, da beim Zugänglichmachen von anonymisierten Daten nicht bekannt ist, mit welchen anderen Daten später Verknüpfungen vorgenommen werden. Je mehr anonymisierte Daten aus den verschiedensten Bereichen zur Verfügung stehen, desto grösser ist das Risiko, dass eine Re-Individualisierung eben doch wieder möglich ist.

6.1.4 Zwischenergebnis

[Rz 34] Aufgrund der Möglichkeiten im Rahmen von Big Data sind Personendaten *konsequenter und effektiver* als bisher zu anonymisieren. Dadurch wird das Risiko einer Re-Individualisierung massiv gesenkt.

[Rz 35] Da eine Re-Individualisierung in der Praxis jedoch nie ausgeschlossen werden kann, ist

Offenbar ein Einzelfallentscheid, digma 2011/1 S. 41.

51 Bruno Baeriswyl, Big Data zwischen Anonymisierung und Re-Individualisierung, S. 47 (in Weber/Thouvenin, zit. in FN 1).

52 Latanya Sweeney, Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3, Pittsburgh, 2000, S. 2 sowie Latanya Sweeney; Weaving Technology and Policy Together to Maintain Confidentiality, Journal of Law, Medicine & Ethics, 1997/25 (nos. 2 & 3) S. 98—110.

53 Philippe Golle, Revisiting the Uniqueness of Simple Demographics in the US Population, Palo Alto Research Center, 2006, S. 1.

zu prüfen, wie diese rechtlich zu beurteilen ist.[54]

6.1.5 Exkurs: Pseudonymisierte Personendaten

[Rz 36] Ergänzend sei hier noch auf *pseudonymisierte Personendaten* hingewiesen. Dabei handelt es sich um Personendaten, bei denen der Personenbezug nicht unwiderruflich entfernt wurde. Es handelt sich somit *nicht* um eine Anonymisierung im Sinne des Datenschutzrechts.[55] Das deutsche Bundesdatenschutzgesetz[56] definiert den Vorgang wie folgt: «Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschliessen oder wesentlich zu erschweren.» Zu denken ist etwa an Laborergebnisse, bei denen der Patientenname durch einen Code ersetzt wird. Wer zukünftig mit diesen Daten arbeitet, kennt nur den Code, kann somit keine Zuordnung zum Patienten machen. Da jedoch die Codierungsstelle nach wie vor den Bezug zu den einzelnen Patienten herstellen kann, ist diese Art der Anonymisierung nicht irreversibel. Die pseudonymisierten Daten sind daher rechtlich grundsätzlich[57] wie *Personendaten*, nicht wie Sachdaten zu behandeln.[58] Etwas anderes gilt nur dann, wenn die Zuordnungsinformationen irreversibel vernichtet werden und die pseudonymisierten Daten wie vorstehenden im Abschnitt 6.1.3 ausgeführt, korrekt anonymisiert sind.[59]

6.2 Big-Data-Analyse anonymisierter Daten — Ziel: Auswertungsergebnis ohne Personenbezug

[Rz 37] Werden rechtmässig und vollständig anonymisierte Daten mittels Big Data analysiert und ist bezüglich der Auswertung weder ein Personenbezug geplant, noch kann sich ein solcher — selbst auch nicht unbeabsichtigt — ergeben, so besteht bei einer solchen Datenbearbeitung zu keinem Zeitpunkt ein Personenbezug. Das Datenschutzrecht kommt daher nicht zur Anwendung.

[Rz 38] Sofern die datenbearbeitende Verwaltungsstelle auf anonymisierte Daten einer *anderen* kantonalen Verwaltungsstelle angewiesen ist, kommt das jeweilige kantonale Statistikrecht zur Anwendung. Je nach Datenbestand ist zu prüfen, ob allenfalls Amts- oder Berufsgeheimnis einer Datenbekanntgabe im Wege stehen.

---

54 S. hinten im Abschnitt 9.

55 Ebenso WP 29/05/2014, S. 3 (zit. in FN 38).

56 §3 Abs. 6a BDSG.

57 Philip Scholz führt dagegen für das deutsche Recht aus, dass jeweils im konkreten Einzelfall und unter Abwägung aller konkreten Umstände — wie bei den anonymisierten Daten — zu prüfen sei, ob ein Personenbezug gegeben sei oder nicht (vgl. N 218 ff. zu §3 Abs. 6a, in Simitis, Kommentar BDSG, 8. Aufl., Frankfurt a. Main, 2014).

58 René Huber, N 6 zu Art. 32, BSK DSG (zit. in FN 31).

59 Robert Bühler, N 22 zu Art. 21, BSK DSG (zit. in FN 31).

6.3 Big-Data-Analyse von Personendaten — Ziel: Auswertungsergebnis ohne Personenbezug

[Rz 39] In den Bereichen Forschung, Planung, Wissenschaft und Statistik ist nicht auszuschliessen, dass Auswertungsergebnisse *vorerst* noch einen Personenbezug aufweisen. Dieser ist jedoch spätestens beim Zugänglichmachen von Resultaten zu eliminieren.

[Rz 40] Forschung, Planung, Wissenschaft und Statistik bilden jedoch nicht Gegenstand des vorliegenden Beitrags.[60]

6.4 Big-Data-Analyse von Personendaten — Ziel: Auswertungsergebnis mit Personenbezug

6.4.1 Die Rechtslage

[Rz 41] Sollen *Personendaten* mittels Big Data Tools mit weiteren Personen- oder Sachdaten zusammen analysiert und ausgewertet werden, um *personenbezogene* Ergebnisse zu erhalten, so ist dafür eine ausdrückliche *formell-gesetzliche* Rechtsgrundlage erforderlich, stehen doch einem solchen Vorgehen insbesondere die folgenden fundamentalen Grundsätze des Datenschutzrechts entgegen:

- Zweckgebundenheit. Die Quelldaten dürfen ausschliesslich für den gesetzlich vorgesehenen Zweck verwendet werden. Big Data Auswertungen erfolgen hingegen zu *anderen*, allenfalls auch *ergebnisoffenen* Zwecken.
- Transparenz/Erkennbarkeit für Betroffene: Jede Datenbearbeitung muss für Betroffene grundsätzlich erkennbar sein.[61] Das ist bei Big Data nicht der Fall, da die Datenbearbeitung eine «Zweitauswertung» darstellt, von welcher der Betroffene nichts erfährt, da sie zu einem beliebigen späteren Zeitpunkt erfolgen kann.
- Datensparsamkeit/Verhältnismässigkeit: Das Verhältnismässigkeitsprinzip verlangt, dass die Verwaltung möglichst wenige Personendaten erhebt und bearbeitet. Verschiedene Kantone sehen das Prinzip der Datensparsamkeit in ihren Datenschutzgesetzen ausdrücklich vor.[62] Big Data steht dem diametral gegenüber, wird doch versucht, möglichst viele Daten zu erheben, zu erschliessen und auszuwerten.
- Missachtung der Rechte Betroffener (Einsicht / Auskunft, Berichtigung): Die betroffene Person muss wissen, welche Verwaltungsstelle welche Daten über sie bearbeitet. Nur so kann sie ihre Rechte bezüglich Auskunft und Einsicht ausüben nur so kann sie überprüfen, ob die über sie vorhandenen Daten richtig sind (falls dem nicht so ist, stehen ihr entsprechende Rechtsbehelfe zur Verfügung.[63] Von Big Data Auswertungen haben die Betroffenen jedoch regelmässig

---

[60] S. dazu vorne Abschnitt 3.2.

[61] §12 IDG-ZH (LS 170.4) sieht unter der Überschrift «Erkennbarkeit der Beschaffung» folgendes vor:«[1] Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein.[2] Bei der Beschaffung von besonderen Personendaten ist der Inhaber der Datensammlung verpflichtet, die betroffene Person über den Zweck ihrer Bearbeitung zu informieren.»

[62] §11 Abs. 1 IDG-ZH (LS 170.4) sieht unter der Überschrift «Vermeidung des Personenbezugs» vor: «Das öffentliche Organ gestaltet Datenbearbeitungssysteme und -programme so, dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind.»Überschrift von §14 IDG-BS (SG 153.260) sowie §13 IDG-BL (SGS 162): «Datenvermeidung und Datensparsamkeit bei IT-Systemen».

[63] Vgl. dazu etwa §15 DSG-ZG (BGS 157.1).

keine Kenntnisse, ihre Rechte können sie daher nicht wahrnehmen.

[Rz 42] Zudem werden bei Big Data in aller Regel auch besonders schützenswerte Personendaten bearbeitet bzw. sind Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben («Persönlichkeitsprofile»). In diesen Fällen verlangen die kantonalen Datenschutzrechte, dass solche Datenbearbeitungen in einem *formellen Gesetz* zu regeln sind.

6.4.2 Zustimmung der Betroffenen?

[Rz 43] Alle kantonalen Datenschutzrechte lassen Datenbearbeitungen (u.a.) dann zu, wenn die betroffene Person diesbezüglich ihre Einwilligung bzw. Zustimmung erteilt.[64] Es stellt sich somit die Frage, ob der Betroffene (vorgängig) seine Einwilligung für (spätere) Big Data Auswertungen erteilen kann. Aus den folgenden Gründen ist dies u.E. *nicht* zulässig:

> (1) Das kantonale Datenschutzrecht sieht in aller Regel vor, dass die Einwilligung *vorgängig*, nur *im Einzelfall* und zudem nur *ausdrücklich* abgegeben werden kann. Dies setzt die Informiertheit des Betroffenen bezüglich der zu erwartenden Datenbearbeitungen voraus. Der Betroffene muss die Folgen seiner Einwilligung überblicken können. Bei Big Data ist jedoch im Vorfeld meist gerade *nicht* klar, was mit den vorhandenen Daten gemacht wird, welche Datenbearbeitungen bzw. Auswertungen vorgenommen werden.

[Rz 44] Da es sich bei Big Data um den Einsatz einer eigentlichen «Carte blanche» handelt, kann der Betroffene u.E. somit grundsätzlich *nicht* vorgängig seine Einwilligung erteilen.

> (2) Die Einwilligung Betroffener ist im öffentlichen Recht grundsätzlich *äusserst kritisch* zu beurteilen,[65] widerspricht sie doch letztlich dem Legalitätsprinzip[66]: Ist die Verwaltung für ihre Aufgabenerfüllung auf Daten angewiesen, ist dies in den entsprechenden Rechtserlassen so vorzusehen bzw. sind die erforderlichen gesetzlichen Grundlagen zu schaffen. Gibt es jedoch keine gesetzliche Grundlage für die Datenbeschaffung, ist letztere grundsätzlich auch nicht zulässig. Hier nun die Figur der Einwilligung des Betroffenen aus dem Hut zu zaubern, ist u.E. grundsätzlich[67] nicht sachgerecht, werden damit doch Datenbearbeitungen ermöglicht, für die es keine gesetzlichen Grundlagen[68] gibt, die somit auch nicht rechtmässig sind. In der Praxis

---

64 Vgl. etwa §8 IDAG-AG (SAR 150.700), Art. 5 DSG-SH (SHR 174.100), Art. 6 DSG-BE (BSG 152.04), Art. 35 LIPAD-GE (RS A 2 08), Art. 6 LPDP-TI (RL 1.6.1.1), §9 Abs. 1/§16 IDG-ZH (LS 170.4), §12/§21 IDG-BS (SG 153.260), §5 DSG-ZG (BGS 157.1).

65 Vgl. dazu Tätigkeitsbericht des DSB des Kantons Zug 2008, S. 8 f.; Meike Kamp/Martin Rost, Kritik an der Einwilligung — Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen, Datenschutz und Datensicherheit/DuD 2013/2 S. 80—84; kritisch auch Spiros Simitis, N 17 zu §4a, Kommentar BDSG, 2014.

66 Vgl. zum Folgenden auch Alexander Rossnagel/Andreas Pfitzmann/Hansjürgen Garstka, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Bonn 2001, S. 73 f.; Spiros Simitis, N 3 zu §4a, BDSG-Kommentar.

67 Ausnahme: Wenn nur der Betroffene — nicht jedoch die Verwaltungsstelle — Vorteile hat, etwa durch Erleichterung oder Beschleunigung von Entscheidprozessen zu seinen Gunsten.

68 Ausser eben der Freizeichnungsklausel der Einwilligung.

nimmt die Verwaltung jedoch oft Zuflucht zum Instrument der Zustimmung.[69] Zu bedenken ist auch, dass Verwaltung und Betroffener sich nicht auf gleicher Augenhöhe begegnen, somit in aller Regel von Freiwilligkeit keine Rede sein kann.[70]

6.4.3 Ein Blick in die Praxis

[Rz 45] Soweit ersichtlich, gibt es bis anhin keine kantonalen gesetzlichen Grundlagen, die Datenbearbeitungen im Bereiche von Big Data *ausdrücklich zulassen*.

[Rz 46] Hingegen gibt es eine neue Bestimmung im Energierecht des Kantons Zug, die Big Data mit Absicht grundsätzlich *verhindert*, hat doch der Zuger Gesetzgeber beim Einsatz von Smart Metering — sehenden Auges[71] — vorgegeben, dass die Energieverbrauchsdaten im Smart Meter selber, somit in den Räumlichkeiten der Kunden, während eines Monats zu *aggregieren* sind und nur diese aggregierten Daten am Ende des Monats durch den Netzbetreiber dem Energielieferanten für die Rechnungsstellung zugestellt bzw. übertragen werden dürfen.[72] Im Übrigen ist jede Weitergabe von Verbrauchs- oder Kundendaten ausdrücklich *untersagt*.[73] Diese Regelung verhindert die Erfassung durch bzw. die Übertragung von Verbrauchswerten im 5-Minuten-Takt an den Energieversorger — wie sonst üblich — und schützt dadurch die Privatsphäre der Energiebezüger.[74] Zu Recht sind davon abweichende vertragliche Vereinbarungen zwischen Netzbetreiber/Energieversorger und Energiebezüger möglich[75] — zu denken ist hier in erster Linie an Unternehmen, die detaillierte und strukturierte Verbrauchs- bzw. Lastdaten benötigen.

6.5 Big-Data-Analyse anonymisierter Daten — Ziel: Auswertungsergebnis mit Personenbezug

[Rz 47] Zu Recht weist Baeriswyl darauf hin, dass es nicht möglich sein sollte, aus anonymisierten Daten wieder einen Personenbezug herzustellen,[76] gibt das Datenschutzrecht doch vor, dass die Anonymisierung von Personendaten gerade so vorzunehmen ist, dass es eben nicht mehr möglich ist, auf die betroffene Person zu schliessen (s. dazu die Ausführungen vorne im Abschnitt 6.1.3 zur Anonymisierung). Ist die Schaffung eines Personenbezugs doch möglich, ist zu prüfen, ob die gesetzlichen Vorgaben bezüglich Anonymisierung eingehalten sind. Ist dies nicht der Fall, sind die Daten durch entsprechende Reduktion von Personenmerkmalen stärker zu anonymisieren.

[Rz 48] In vielen Fällen ermöglicht es Big Data jedoch, selbst aus *rechtskonform anonymisierten* Daten nachträglich wieder einen Personenbezug herzustellen. Das ist insbesondere dann der Fall, wenn anonymisierte Daten aus einer genügend grossen Anzahl unterschiedlicher Quellen und

---

69 Insbesondere im Sozialbereich, wo Betroffene der Verwaltung «freiwillig» eigentliche Blankovollmachten zur Datenbeschaffung erteilen müssen.

70 Vgl. Näheres dazu: Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Zug 2008, S. 8 f.

71 Vgl. dazu Bericht und Antrag der vorberatenden Kommission des Kantonsrats des Kantons Zug vom 28. November 2014 betr. Änderung des Energiegesetzes (Vorlage Nr. 2433.3/Laufnummer 14837).

72 §4a Abs. 4 ZG-Energiegesetz (BGS 740.1).

73 §4a Abs. 3 ZG-Energiegesetz (BGS 740.1).

74 Näheres dazu im Tätigkeitsbericht des Datenschutzbeauftragten des Kantons Zug 2012, S. 5 sowie 2013, S. 24.

75 §4a Abs. 6 ZG-Energiegesetz (BGS 740.1).

76 Bruno Baeriswyl, Big Data zwischen Anonymisierung und Re-Individualisierung, S. 51 (in Weber/Thouvenin, zit. in FN 1).

Bereiche ausgewertet werden. Bei einer solchen Re-Individualisierung — somit dem Herstellen eines Bezugs zu den ursprünglich betroffenen Personen — handelt es sich um die Bearbeitung von Personendaten. Diese Bearbeitung unterliegt ohne weiteres dem Datenschutzrecht und deren Rechtmässigkeit ist aufgrund der anwendbaren kantonalen Datenschutzbestimmungen zu beurteilen.

[Rz 49] Sofern der Datenbearbeiter der Quelldaten seine Pflichten bezüglich der rechtmässigen Anonymisierung erfüllt hat, liegt es u.E. — jedenfalls im hier zu diskutierenden kantonalen Umfeld — nicht mehr in seiner Verantwortung, wie allfällige kantonale Verwaltungsstellen *später* mit seinen rechtskonform anonymisierten Daten umgehen. Verantwortlicher Datenbearbeiter ist diesfalls nun diejenige Verwaltungsstelle, die aufgrund von Big Data-Analysen *einen Personenbezug* herstellt.

6.6 Hinweise zur Herkunft der Quelldaten

6.6.1 Öffentlich bzw. frei zugängliche Daten

[Rz 50] Soweit Sachdaten oder anonymisierte Daten publiziert bzw. frei zugänglich sind, darf die Verwaltungsstelle solche für allfällige Big Data Analysen heranziehen.[77] Zu denken ist etwa an veröffentlichte statistische Daten oder «Open Government Data»[78].

6.6.2 Amtsintern vorhandene Daten

[Rz 51] Verfügt die Verwaltungsstelle intern über eigene Datenbestände an Sachdaten oder anonymisierten Daten, darf sie diese zur Erfüllung ihrer gesetzlich vorgeschriebenen Aufgaben für allfällige Big Data Analysen nutzen.

[Rz 52] Anders sieht es bezüglich Personendaten aus. Diese dürfen nur dann für Big Data Analysen verwendet werden, wenn die Nutzung dem ursprünglichen Erhebungszweck entspricht oder eine entsprechende ausdrückliche gesetzliche Grundlage dies zulässt. In allen übrigen Fällen dürfen selbst amtsintern vorhandene Personendaten nicht für Big Data Auswertungen genutzt werden.

6.6.3 Kantonsintern vorhandene Daten

[Rz 53] Soweit nicht Amts-, Berufs- oder Spezialgeheimnisse[79] bzw. Schweigepflichten dem entgegenstehen, dürfen Sachdaten und anonymisierte Daten — nicht aber Personendaten — *anderer* kantonsinterner Verwaltungsstellen für allfällige Big Data Analysen herangezogen werden.

---

77 Unter Beachtung allfällig vorhandener Nutzungsbestimmungen.

78 Vgl. dazu etwa das «Open Government Data-Pilotportal» von Bund und verschiedener Kantone («http://opendata.admin.ch»).

79 Steuergeheimnis, Sozialhilfegeheimnis.

6.6.4 Datenbezug von kantonsexternen Verwaltungsstellen

[Rz 54] Sachdaten und anonymisierte Daten — nicht aber Personendaten — von Bund bzw. von anderen Kantonen dürfen für Big Data Auswertungen übernommen werden, sofern die fraglichen externen Stellen zur Datenbekanntgabe befugt sind.

6.6.5 Datenbezug von Unternehmen?

[Rz 55] In- oder ausländische Unternehmen verfügen über beliebige Bestände an Kundendaten. Daten aus verschiedenen Sachbereichen könnten auch für die Verwaltung von grossem Interesse sein. Zu denken ist etwa an Kommunikationsdaten. Darf die Verwaltung Sach- oder Personendaten auf dem «Datenmarkt» kaufen?[80] Dazu ein Beispiel aus den Niederlanden: Im Jahr 2011 kauften regionale und lokale niederländische Polizeibehörden von der Firma TomTom — dem weltweit grössten Navigationsgerätehersteller — Bewegungsprofile von niederländischen TomTom-Kunden, um Verkehrskontrollen zu optimieren.[81,82]

[Rz 56] Insbesondere müssen die beiden folgenden Voraussetzungen erfüllt sein: Die Unternehmung muss berechtigt sein, über die fraglichen Daten entsprechend verfügen zu dürfen und die Verwaltungsstelle darf den Datenbezug nur für die Erfüllung ihrer gesetzlich vorgesehenen Aufgaben nutzen.

[Rz 57] Im vorstehenden Beispiel aus den Niederlanden stand denn (wohl zu Recht) nicht die Polizei in der Kritik, sondern das private Unternehmen, das nicht berechtigt war, die fraglichen Daten in dieser Art und Weise den Behörden zu verkaufen, hatte es doch die Kundschaft diesbezüglich weder informiert, noch deren ausdrückliche Einwilligung erhalten.

7 Fazit

[Rz 58] Big Data in der kantonalen Verwaltung a) ist *zulässig*, wenn

- ausschliesslich Sachdaten bearbeitet werden (und es sich auch bei allfälligen späteren Verknüpfungen ausschliesslich um Sachdaten handelt)
- eine ausdrückliche formell-gesetzliche Regelung vorhanden ist
- (allenfalls: die informierte und ausdrückliche Zustimmung sämtlicher Betroffenen liege vor und der Eingriff in die Privatsphäre wiege nicht schwer. S. dazu jedoch die kritischen Ausführungen vorne[83])

b) *kann zulässig sein* im Bereich von

- Forschung, Planung, Wissenschaft und Statistik

---

80 Nicht Thema ist hier die Datenbekanntgabe aufgrund ausdrücklicher gesetzlicher Grundlagen (z.B. Bezug von Kommunikationsdaten von Providern im Rahmen von Strafverfahren).

81 Vgl. dazu den Untersuchungsbericht der niederländischen Datenschutzbehörde (College Bescherming Persoonsgegevens/CBP) vom 20. Dezember 2011, der zum Schluss kam, dass TomTom ohne Zustimmung der Kundschaft Personendaten verkauft hatte: «Official investigation by the College Bescherming Persoonsgegevens/CBP into the processing of geolocation data by TomTom N.V.».

82 Ergänzend: Nach Bekanntwerden dieses Datenverkaufs in den Medien hatte die Firma TomTom ein datenschutzrechtliches Problem, da die Kundschaft über Speicherung und Datenweitergabe nicht korrekt informiert worden war, zudem die Daten ungenügend anonymisiert waren.

83 Vgl. die Ausführungen im Abschnitt 6.4.1.

- Strafverfolgung

c) ist in allen übrigen Fällen *unzulässig bzw. benötigt*:

- eine ausdrückliche formell-gesetzliche Rechtsgrundlage

8 Empfehlungen

[Rz 59] Es ist davon auszugehen, dass früher oder später auch kantonale Behörden auf die Analyse-Möglichkeiten von Big Data zugreifen wollen. Sind dabei Personendaten tangiert,[84] ist diesbezüglich eine *explizite formell-gesetzliche Rechtsgrundlage* erforderlich, handelt es sich doch einerseits um Ausnahmeregelungen zum Datenschutzrecht,[85] andererseits werden in aller Regel auch besonders schützenswerte Personendaten bzw. Persönlichkeitsprofile bearbeitet.

[Rz 60] Nicht empfehlenswert ist die Schaffung eines allgemeinen und umfassenden kantonalen «Big Data Gesetzes». Ein solches müsste zu abstrakt formuliert werden, die erforderliche Konkretisierung des Regelungsgegenstandes bzw. der zulässigen Datenbearbeitungen würde fehlen.

[Rz 61] Vielmehr müsste Big Data u.E. in den *betroffenen Rechtsgebieten* besonders geregelt — allenfalls auch ausdrücklich ausgeschlossen[86] — werden. Explizit zu regeln wären insbesondere: Zweck der Datenbearbeitung, Herkunft bzw. Bezug[87] von Daten, Einsichtsrechte Betroffener sowie Nutzung, Weitergabe bzw. Veröffentlichung von Auswertungen.

[Rz 62] Der Staat darf bei einer allfälligen gesetzlichen Regelung von Big Data nicht alles zulassen, was technisch möglich ist. Vielmehr ist er, wie stets, an die verfassungsmässigen Grundprinzipien, insbesondere an das Verhältnismässigkeitsprinzip gebunden.

[Rz 63] Aus grundsätzlichen Überlegungen hat der Staat im vorliegenden Bereich grundsätzlich *grosse Zurückhaltung* an den Tag zu legen, ist doch der Schutz der Privatheit der Bürgerinnen und Bürger in einem freiheitlichen demokratischen Staat von zentraler Bedeutung.

[Rz 64] Es ist zudem erforderlich, die Aspekte von Big Data im Rahmen eines kantonalen *Gesamtkonzepts* bzw. einer *Strategie* zukunftsgerichtet anzugehen und dabei insbesondere auch die datenschutzrechtlichen Aspekte bzw. Risiken genauer zu beleuchten und zu bewerten.

9 Abschliessend — hier besteht Klärungsbedarf

[Rz 65] Gibt es in Zeiten von Big Data noch «harmlose», frei zu verwendende Informationen? Anders gefragt: Ist die im Gesetz festgelegte scharfe Trennung — mit den entsprechenden rechtlichen Konsequenzen — von Personendaten und Sachdaten im Hinblick auf Big Data noch sachgerecht?[88] Oder besteht letztlich das grundsätzlich gleiche Schutzbedürfnis für sämtliche Daten, unabhängig davon, ob wir zu einem bestimmten Zeitpunkt einen Bezug zu einer Person machen

84 Quelldaten oder Auswertungsdaten.

85 Verstösst doch Big Data in grundsätzlicher Weise u.a. gegen das Zweckänderungsverbot der Datenbearbeitung, gegen das Prinzip der Datensparsamkeit und gegen das Transparenzprinzip.

86 Wie im Energierecht des Kantons Zug, vgl. dazu vorne im Abschnitt 6.4.3.

87 Nur verwaltungsintern — oder auch bei Privaten?

88 Vgl. Thomas Probst, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Person im Datenschutzrecht, AJP 2013 S. 1423—1436, S. 1423.

können oder nicht?

[Rz 66] Diese Frage müsste im Rahmen der geplanten Revision des Datenschutzrechts des Bundes näher untersucht und geklärt werden.[89]

Dr. iur René Huber, Datenschutzexperte, Inhaber der Firma Recht + Informatik in Zürich, von 1999 bis 2014 Datenschutzbeauftragter des Kantons Zug, Autor von Fachbeiträgen (u.a. Basler Kommentar zum Datenschutzgesetz, Kommentator der Art. 26—32 DSG).

[89] Der Bundesrat will den Datenschutz in der Schweiz stärken. Er hat deshalb am 1. April 2015 eine Revision des Datenschutzgesetzes beschlossen und das EJPD beauftragt, ihm unter Berücksichtigung der derzeit laufenden Datenschutzreformen in der EU und beim Europarat bis spätestens Ende August 2016 einen Vorentwurf für eine Revision des DSG zu unterbreiten (alles Nähere dazu findet sich auf der Website des EDÖB, vgl. auch Medienmitteilung des Bundesrates, «Der Datenschutz soll gestärkt werden», 1. April 2015).