www.jusletter-it.eu

Michal Cichocki

Big Data und Datenschutz: Ausgewählte Aspekte

The present article highlights selected data protection aspects of Big Data technologies. The author mainly analyzes legal issues as well as possible solutions in the context of a possible re-identification of anonymized personal data and the principles of data processing of purpose limitation, proportionality and consent.

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

Citation: Michal Cichocki, Big Data und Datenschutz: Ausgewählte Aspekte, in: Jusletter IT 21 May 2015

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

Inhaltsübersicht

1 Anwendungsmöglichkeiten

[Rz 1] Big Data ist bereits vor einiger Zeit dem Schatten der Fachmedien entflohen und als Schlagwort in das Rampenlicht der Mainstreampresse gerückt. Dabei ist jeweils vom Öl des 21. Jahrhunderts[1], vom Rohstoff der Gegenwart[2], vom neuen Goldrausch[3] oder aber vom gläsernen Menschen, Totalüberwachung und Big Brother[4] die Rede.

[Rz 2] Trotz dieser plakativen Anpreisung scheinen Big Data Technologien zu halten, was sie versprechen; die neuen Möglichkeiten sind beeindruckend: Mit Big Data könnten Behörden die Ausbreitung von Epidemien vorhersagen und Spitäler wären in der Lage, bis anhin verborgene Nebeneffekte bei Medikamenten aufzudecken[5]. Unternehmen könnten schneller auf Marktveränderungen reagieren, ihre Wettbewerbsfähigkeit steigern, neue Produkte entwickeln oder

1 Dirk Helbing, Sozial orientierte Technologie, NZZ vom 19. August 2013 (online).

2 Stefan Heuer, Im Goldrausch, NZZ Folio vom Mai 2013.

3 Thomas Fischermann und Götz Hamann, Wer hebt das Datengold? Zeit vom 6. Januar 2013 (online).

4 Hendrik Ankenbrand und Britta Beeger, Der gläserne Mensch, FAZ vom 9. Januar 2013 (online).

5 Resolution of Big Data, 36th International Conference of Data Protection and Privacy Commissioners, Mauritius 2014.

bestehende Angebote verbessern[6]. Autofahrer könnten wegen ihres (gefährlichen) Fahrstils von bestimmten Leistungen ihrer Versicherer ausgeschlossen werden[7]. Die Polizei könnte Verbrechen erkennen, bevor sie stattfinden und vorbeugend eingreifen[8], während Kriminelle genauer wüssten wann sie wo, wie einbrechen könnten[9].

[Rz 3] Mit Big Data Technologien können also vor allem neue Zusammenhänge in fast allen Bereichen des Lebens entdeckt, detailliert analysiert und künftige Ereignisse vorhergesagt werden[10]: durch die Datafizierung[11] unseres Alltags, namentlich das Hinterlassen einer digitalen Datenspur durch die tägliche Nutzung von Telefon und Internet beim Kommunizieren, GPS-Navigationsgeräten beim Fortbewegen, Kreditkarten beim Einkaufen aber auch durch die gesetzlich vorgesehene Erfassung bzw. Veröffentlichung von Daten im Rahmen von Open-Government-Data können Daten zu Hobbies, Einkaufsverhalten, Arbeitswegen, Freundeskreis etc. durch Private und das Gemeinwesen gesammelt, ausgetauscht, verknüpft, weitergegeben oder verkauft werden[12].

2 Begriff

[Rz 4] Genauso zahlreich wie die verschiedenen möglichen Auswirkungen und Anwendungsgebiete, ist auch die Bedeutung des Begriffs selber: Big Data als Schlagwort wird oft unterschiedlich verwendet. Einerseits werden damit Technologien zum Beschaffen und Auswerten sehr grosser Datenmengen bezeichnet[13]. Andererseits wird auf die Art und Herkunft von Daten Bezug genommen:

- «*Big Data ist die Ansammlung möglichst vieler Daten, die aus möglichst vielen Datenquellen zur Verfügung stehen*»[14] — oder die Verschmelzung der Möglichkeiten des «*Data Warehousing*[15]» mit «*Data Mining*[16]» und dem «*Cloud Computing*[17]»[18].
- «*Big Data bezeichnet die wirtschaftlich sinnvolle Gewinnung und Nutzung entscheidungsrelevanter Erkenntnisse aus qualitativ vielfältigen und unterschiedlich strukturierten Informationen, die*

6 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., BITKOM Big Data im Praxiseinsatz — Szenarien, Beispiele, Effekte, 2012, S. 8.

7 Wer hebt das Datengold? Zeit, a.a.O.

8 Daniel Schurter, «Precobs» — Verbrechen erkennen, bevor sie passieren — so funktioniert die Software der Schweizer Polizeien, Watson.ch vom 2. Oktober 2014.

9 Der gläserne Mensch, FAZ, a.a.O.

10 Resolution of Big Data, a.a.O., p.1.

11 Die Umwandlung von Aspekten des Alltags in computerisierte Daten.

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

13 Edd Dumbill, What is big data? An introduction tot he big data landscape, 11. Januar 2013, http://radar.oreilly.com/2012/01/what-is-big-data.html.

14 Bruno Baeriswyl, «Big Data» ohne Datenschutz — Leitplanken, in: Digma — die Zeitschrift für Datenrecht und Informationssicherheit 2013, S. 14.

15 Prozess zur Bewirtschaftung und Auswertung eines Datenlagers (Data Warehouse).

16 Die systematische Anwendung statistischer Methoden auf einen Datenbestand mit dem Ziel, neue Muster zu erkennen.

17 Speichern von Daten in einem entfernten Rechenzentrum, aber auch die Ausführung von Programmen, die nicht auf dem lokalen Rechner installiert sind.

18 Bruno Baeriswyl, a.a.O., S. 14.

einem schnellen Wandel unterliegen und in bisher ungekanntem Umfang anfallen»[19].

- «*Big Data is a term which refers to the enormous increase in access to and automated use of information. It refers to the gigantic amounts of digital data controlled by companies, authorities and other large organisations which are subject to extensive analysis on the use of algorithms*»[20].
- «*Big Data lässt sich im Wesentlichen durch vier Merkmale definieren, welche aufgrund ihrer englischen Bezeichnung als die vier «V's» bezeichnet werden: Big Data sind grosse Datenmengen (Volume), die mit hoher Geschwindigkeit (Velocity) verarbeitet werden. Ein drittes Merkmal ist die unterschiedliche Beschaffenheit oder Vielfalt (Variety) der Daten. [...] Das vierte Merkmal ist der Mehrwert (Value), welcher mit der Datenanalyse geschaffen wird*»[21].

[Rz 5] Im Ergebnis können m.E. den genannten Definitionen folgende Wesensmerkmale für den Begriff von Big Data entnommen werden:

[Rz 6] Big Data sind (i) jede denkbare Art von Angaben[22] zu beliebigen Themen, (ii) in gigantischem und stetig zunehmendem Umfang, (iii) die aus verschiedenen Quellen stammen sowie miteinander verknüpfbar sind, (iv) nur noch mit Hilfe hochleistungsfähiger Technologien bearbeitbar und (v) zur Verwendung für unbestimmte Zwecke geeignet sind.

[Rz 7] Der Begriff Big Data bleibt aber dynamisch. Er wird sich, abgesehen von einer — unwahrscheinlichen — künftigen Legaldefinition, wohl kaum abschliessend definieren lassen. Zu rasant ist der technologische Fortschritt, zu wenig vorhersehbar sind künftige Entwicklungen: Sobald das Internet der Dinge[23], Smart Homes[24], Werables, künstliche Intelligenz[25] etc. fester Bestandteil unseres Alltags geworden sind, könnte sich der Begriff «Big Data» erneut wandeln.

3 Anwendbarkeit der Datenschutzgesetzgebung

[Rz 8] Die schweizerische Datenschutzgesetzgebung wurde 1993 in Kraft gesetzt. Sie stammt damit aus einer Zeit lange vor Big Data. Ungeachtet dessen findet das Bundesgesetz über den Datenschutz (DSG) auch auf Big Data Anwendung, sobald Personendaten im Sinne von Art. 3 lit. a DSG bearbeitet werden (die kantonalen Datenschutzgesetze knüpfen an dieselben Merkmale an und sind auf die Bearbeitung von Personendaten durch Kantonsbehörden anwendbar).

[Rz 9] Die Legaldefinition der Personendaten gemäss Art. 3 lit. a DSG umfasst drei Wesensmerkmale: (i) sämtliche Angaben (d.h. jede Art und Form von Informationen oder Aussagen), die (ii) einen Bezug zu einer natürlichen oder juristischen Person (sog. Personenbezug) haben und (iii) die Bestimmtheit oder Bestimmbarkeit (d.h. die Möglichkeit der (Re-)Identifizierung) dieser Per-

---

[19] BITKOM, a.a.O., S. 7.

[20] International Working Group on Data Protection in Telecommunications (IWGDPT), Working Paper on Big Data and Privacy — Privacy principles under pressure in the age of Big Data analytics, 55th Meeting, 5—6 May 2014, Skopje, p. 1.

[21] EDÖB, Erläuterungen zu Big Data, a.a.O.

[22] Damit ist alles, was mittels Beobachtung, Messung, Aufnahme etc. gewonnen werden kann, gemeint. Dies beschränkt sich nicht auf «Daten» bzw. «Personendaten» im datenschutzrechtlichen Sinne (vgl. Ziff. 3 hienach).

[23] Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgaben für den Besitzer/Nutzer erledigen können.

[24] Intelligente Vernetzung von Haustechnik und Haushaltsgeräten (zum Beispiel Lampen, Heizung, etc.), als auch die Vernetzung von Komponenten der Unterhaltungselektronik.

[25] Gartner identifies the Top 10 Strategic Technology Trends for 2015, 8. Oktober 2014, http://www.gartner.com/newsroom/id/2867917.

son[26]. Bei Personendaten «*kann es sich sowohl um Tatsachenfeststellungen als auch um Werturteile handeln. Unerheblich ist, in welcher Form die Informationen auftreten (etwa als Zeichen, Wort, Bild, Ton oder eine Kombination davon) und wie der Datenträger beschaffen ist. Entscheidend ist, dass sich die Angaben einer oder mehreren Personen zuordnen lassen*»[27].

[Rz 10] Der Begriff des Bearbeitens ist weit[28] zu verstehen und umfasst jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren (Art. 3 lit. e DSG). Damit ist der Begriff des Bearbeitens an sich insofern unproblematisch und immer dann zu bejahen, sobald mit Big Data «etwas gemacht» (d.h. Beschaffen/Sammeln, Analysieren, Bekanntgeben etc.) wird. Entscheidend ist, ob sich das Bearbeiten auf Personendaten im vorgenannten Sinn bezieht. Wird dies bejaht, ist das DSG anwendbar, was eine ganze Reihe an Rechten und Pflichten mit sich bringt: bspw. Beachtung der Bearbeitungsgrundsätze (Art. 4 ff. DSG), insbesondere bei grenzüberschreitenden Bekanntgaben (Art. 6 DSG), Auskunftsrecht beim Vorliegen von Datensammlungen (Art. 8 ff. DSG), Anmeldung einer Datensammlung (Art. 11a DSG), Rechtfertigungsgründe (Art. 13 ff. DSG), Strafbestimmungen (Art. 34 f DSG) etc.

[Rz 11] Nachfolgend werden ausgewählte Aspekte von Big Data auf ihre Vereinbarkeit mit der geltenden schweizerischen Datenschutzgesetzgebung untersucht und Lösungsvorschläge für datenschutzrechtliche Probleme präsentiert. Dabei werden insbesondere zwei Problemkreise untersucht: die Re-Identifizierung (Ziff. 4) sowie die komplexe Bearbeitung von grossen Mengen von Personendaten (Ziff. 5 bis 8).

4 Re-Identifizierung

4.1 Ausgangslage und Problematik

[Rz 12] Im Zusammenhang mit Big Data wird oft argumentiert, dass in vielen Fällen gar keine Personendaten im Sinne des DSG bearbeitet würden. Demnach sei die Datenschutzgesetzgebung gar nicht anwendbar[29]. Wie erwähnt, umfasst der Begriff Big Data jede denkbare Art von Angaben (vgl. Ziff. 2 hievor). Aus diesem Grund muss im Einzelfall geprüft werden, ob Personendaten gemäss Art. 3 lit. a DSG bearbeitet werden und ob folglich das DSG anwendbar ist oder nicht.

[Rz 13] Keine Personendaten werden dann bearbeitet, wenn reine Sachdaten (d.h. Angaben, bei denen von vornherein kein Personenbezug existierte) bzw. anonymisierte Daten (d.h. Angaben, bei denen sämtliche Identifikationsmerkmale einer Person entfernt wurden) beschafft, analysiert etc. werden und Rückschlüsse auf betroffene Personen gänzlich ausgeschlossen sind. Diesfalls ist die (Wieder)Herstellung des Personenbezugs und damit die Bestimmbarkeit bzw. die Re-Identifizierung derjenigen Person, auf welche sich die bearbeiteten Daten beziehen, nicht möglich: bspw. scheinen Temperaturmessungen, Windstärken und weitere Wetterphänomene aus Sensoren auf Häuserfassaden sowie Wettersatelliten (sog. sensor-generated data) zwecks Auswer-

[26] David Rosenthal, in: David Rosenthal/Yvonne Jöhri, Handkommentar DSG, Zürich 2008, Art. 3 lit. a, N 6 und 18.

[27] BGE 136 II 508 S. 514, Erw. 3.2.

[28] Rosenthal, a.a.O., Art. 3 lit. e, N 63.

[29] EDÖB, Erläuterungen zu Big Data, a.a.O.

tung für Wettervorhersagen[30] unproblematisch. Diese reinen Sachdaten (Angaben) beziehen sich von vornherein nicht auf eine natürliche oder juristische Person, weswegen ein Personenbezug sowie eine Re-Identifizierung nicht möglich sind. Das DSG ist somit nicht anwendbar.

[Rz 14] Aus datenschutzrechtlicher Sicht ist dann Vorsicht geboten, wenn solche an sich «unproblematischen» Daten mit weiteren (anonymisierten) Daten verknüpft werden: Würden nun die vorgenannten «Wetterdaten» (und weitere Sachdaten) mit bspw. anonymisierten Schadensmeldungen (ohne Ortsangaben) von Versicherungen etc. verknüpft, wäre die Wiederherstellung des Personenbezugs sowie eine Re-Identifizierung der anonymisierten Daten und damit die Anwendbarkeit des DSG nicht mehr ausgeschlossen (vgl. weiter unten): Der Ausschluss der Re-Identifizierung ist umso weniger möglich, je mehr Daten aus unterschiedlichen Quellen verknüpft werden — trotz vermeintlicher Anonymisierung[31]. Mit anderen Worten ist die Wahrscheinlichkeit einer Re-Identifizierung der von einer Datenbearbeitung betroffenen Personen umso grösser, je mehr Daten bearbeitet werden[32].

[Rz 15] Zur Illustrierung dieses Phänomens werden gerne folgende zwei Studien aufgegriffen: Einerseits hat sich gezeigt, dass zwischen 61% und 87% der US-amerikanischen Bevölkerung mittels Angaben zum Geschlecht, zum vollständigen Geburtsdatum und zur fünfstelligen Postleitzahl eindeutig identifizierbar waren. Andererseits konnten anonyme Gen-Sequenzen aus öffentlich zugänglichen Forschungsdatenbanken durch Verknüpfung mit wenigen weiteren Daten re-Identifiziert werden[33].

[Rz 16] Zurückkommend auf das oben genannte Beispiel, wäre es mindesten theoretisch denkbar, dass aufgrund des Wetterphänomens, des Zeitpunkts und der Art des gemeldeten Schadens (z.B. Hochwasserschaden) der Wohnort der betroffenen Person eingegrenzt werden könnte. Wenn die Meldung auch das Geschlecht und das Geburtsdatum enthalten würde, wäre eine Re-Identifizierung der von einem Unwetter betroffenen Person gemäss oben genannter US-Studie im Einzelfall wohl möglich und die Datenschutzgesetzgebung könnte damit auf die eingesetzte Big Data Technologie anwendbar sein.

4.2 Voraussetzungen des Bundesgerichts

[Rz 17] Die Frage nach der Bestimmbarkeit und der daraus folgenden Re-Identifizierung der betroffenen Person ist zentral für die Anwendung des DSG auf Big Data. Wie gesagt, steigt die Wahrscheinlichkeit der Re-Identifizierung mit zunehmender Datenmenge. Gemäss Bundesgericht genügt jedoch nicht bereits jede theoretische Möglichkeit zur Re-Identifizierung um im datenschutzrechtlichen Sinn einen Personenbezug und damit die Anwendung des DSG zu bejahen. Ist der Aufwand im Einzelfall gemäss allgemeiner Lebenserfahrung so gross (also übermässig), dass nicht damit gerechnet werden muss, dass ihn ein Datenbearbeiter auf sich nehmen würde, ist die Re-Identifizierung zu verneinen. Dabei sind die Möglichkeiten der Technik mit zu berück-

30 Steve Hamm, How Big Data Can Boost Weather Forecasting, vom 27. Februar 2013 in Wired, http://www.wired.com/2013/02/how-big-data-can-boost-weather-forecasting/.

31 Thilo Weichert, Big Data und Datenschutz, Beitrag für das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, 2013, S. 16.

32 Rolf H. Weber, Big Data, Sprengkörper des Datenschutzrechts?, in: Jusletter IT 11. Dezember 2013, S. 3.

33 Rolf H. Weber, Big Data: Rechtliche Perspektive, in: Rolf H. Weber / Florent Thouvenin (Hrsg.) Big Data und Datenschutz — Gegenseitige Herausforderungen, ZIK 59, 2014, S. 20.

sichtigen. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Re-Identifizierung hat[34].

[Rz 18] Aufgrund des technischen Fortschritts ist die bundesgerichtliche Voraussetzung des nicht übermässigen (technischen) Aufwands zur Bestimmbarkeit bzw. Re-Identifizierung zunehmend zu bejahen. Einschränkend könnte der Umstand sein, dass hinsichtlich der konkret eingesetzten Big Data Technologien kaum Transparenz existiert: Die verwendeten Analysemethode und -technologien sind eine Blackbox; Unternehmen betrachten ihre Analysealgorithmen als Betriebs- und Geschäftsgeheimnis. Eine unabhängige Überprüfung der Methoden und Ergebnisse ist faktisch oft nicht möglich[35]. Deswegen könnte allenfalls eine gewisse (Rest)Ungewissheit hinsichtlich der Voraussetzung des nicht übermässigen Aufwands verbleiben. Das Interesse eines Datenbearbeiters an einer Re-Identifizierung aufgrund der Bearbeitung einer gigantischen Anzahl unterschiedlicher Daten Schlüsse auf Personen(daten) ist dagegen regelmässig zu bejahen[36]; komplett anonymisierte Daten sind für Big Data nur von beschränktem Interesse, da sie nur generelle Aussagen ermöglichen würden[37]. Im Ergebnis könnte die Anwendbarkeit des DSG auf Big Data Technologien tendenziell bereits in einer frühen «Bearbeitungsphase» bejaht werden.

4.3 Datensammlungen ohne Re-Identifizierung — trotzdem potentiell problematisch

[Rz 19] Auch vor der Bejahung einer nicht übermässig aufwendigen Bestimmbarkeit bzw. Re-Identifizierung können datenschutzrechtlich «unproblematische» Daten, die mittels Big Data Technologien bearbeitet werden, problematisch werden: Je nach dem, wie oder womit sie verknüpft werden, wird eine Re-Identifizierung anonymisierter Daten ermöglicht[38] (vgl. Beispiel gemäss Ziff. 4.1 hievor). Andererseits ist in der Phase vor der Re-Identifizierung das DSG nicht anwendbar. Folglich müssen datenschutzrechtliche Prinzipien zum Schutz von Persönlichkeitsrechten hier nicht eingehalten werden; damit entfällt der der Datenschutzgesetzgebung inhärente präventive Schutz. Dies könnte sich negativ auswirken[39]: Denkbar wäre es, dass die Schutzmechanismen des DSG zu spät greifen würden, weil die Ursache für eine Persönlichkeitsrechtsverletzung bereits vorher gesetzt wurde oder nachträglich nicht mehr korrigiert werden kann.

---

34 BGE 136 II 508 S. 514, Erw. 3.2.

35 Thilo Weichert, a.a.O., S. 17.

36 Rolf H. Weber, Big Data, Sprengkörper des Datenschutzrechts?, in: Jusletter IT 11. Dezember 2013, S. 3.

37 Rolf H. Weber/Dominic N. Staiger, Vertragsgestaltung rund um Big Data, in: Weber/Thouvenin (Hrsg.) Big Data und Datenschutz — Gegenseitige Herausforderungen, ZIK 59, S. 158.

38 Peter Schaar, Datenschutz in Zeiten von Big Data, Datenschutz in Zeiten von Big Data, in: HDM Praxis der Wirtschaftsinformatik, Dezember 2014, Band 51, Ausgabe 6, S. 846.

39 Bruno Baeriswyl, a.a.O., S. 15.

4.4 Lösungsansätze

4.4.1 Datenbearbeitungsrecht

[Rz 20] Denkbar wäre die Einführung eines «Datenbearbeitungsrechts»[40] als neue regulatorische Massnahme. Dieses wäre nicht auf Personendaten beschränkt. Es könnte Bearbeitungsvorschriften für alle Arten von Daten (Angaben) vorsehen, was eine allfällige künftige Persönlichkeitsverletzung minimiert oder sogar verhindern könnte.

[Rz 21] In diesem Zusammenhang wäre ein Blick auf die Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung; ISchV) als mögliches Vorbild für ein künftiges «Datenbearbeitungsrecht» denkbar. Die ISchV bezweckt zwar nicht den Schutz von Persönlichkeitsrechten oder der informationellen Selbstbestimmung. Sie schützt primär das Landesinteresse (Art. 1 Abs. 1 ISchV): «*Der Informationsschutz bezweckt die Sicherheit gewisser Informationen im Interesse des Landes zu gewährleisten; dies unabhängig davon, ob diese Informationen auch Personendaten enthalten*»[41]. Interessant ist aber, dass die ISchV unter anderem Bestimmungen zur Bearbeitung von Informationen festlegt. Während der Begriff des Bearbeitens gemäss Art. 3 lit. c ISchV mit demjenigen von Art. 3 lit. e DSG vergleichbar ist, wird der Begriff der Informationen weiter gefasst als jener der Personendaten: Gemäss Art. 3 lit. a ISchV sind unter Informationen sämtliche Aufzeichnungen auf Informationsträgern und mündliche Äusserungen zu verstehen.

[Rz 22] Per Analogiam könnten gewisse Bearbeitungsvorschriften aufgestellt werden, die für alle Daten (nicht nur Personendaten) bereits frühzeitig greifen, d.h. bevor die Schwelle zur Anwendung des DSG überschritten würde. Die Frage nach dem Inhalt solcher Bearbeitungsvorschriften wäre zu diskutieren. Allerdings würden sich neue Administrativaufwände ergeben, was wenig wirtschaftsfreundlich wäre.

4.4.2 Zweckbezogene Anwendung des DSG

[Rz 23] Die Anwendung des DSG auf Big Data Technologien könnte am Zweck bzw. Ergebnis der Datenbearbeitung anstatt alleine am Merkmal der Bearbeitung von Personendaten anknüpfen:

- Bezweckt die eingesetzte Big Data Technologie von Anfang an die Bearbeitung von Personendaten, so dass eine Re-Identifizierung im Sinne der oben genannten Voraussetzungen des Bundesgerichts möglich wäre, könnte die Anwendung des DSG umfassend bejaht werden, also bereits ab Beschaffung der Daten. Dabei wäre unerheblich, ob reine Sach- bzw. anonymisierte Daten oder bereits Personendaten beschafft und in welchem Zeitpunkt die Re-Identifizierung erfolgen würden (vgl. Ziff. 5 ff. zu den Rechtsfolgen).
- Dasselbe könnte für den Fall gelten, bei denen Personendaten zwar nicht dem primären Zweck der eingesetzten Big Data Technologie entspringen, jedoch quasi als Nebenprodukt daraus resultieren.
- Schliesslich verbleibt die Bekanntgabe von Sachdaten oder anonymisierten Personendaten an Dritte. Diesfalls wäre das DSG grundsätzlich dann anwendbar, wenn der weitergebende Datenbearbeiter wüsste oder wissen müsste, dass der empfangende Datenbearbeiter aufgrund

[40] Bruno Baeriswyl, a.a.O., S. 15.

[41] Erläuterungen zur Verordnung über den Schutz von Informationen des Bundes, Stand 12. April 2007, S. 2.

seiner eigenen oder weiterer Daten eine Re-Identifizierung vornehmen könnte[42].

[Rz 24] Inwiefern dies praktikabel wäre, bleibt angesichts der oft im Voraus unbekannten Zwecke von Big Data Technologien jedoch offen.

4.4.3 Entscheid durch Datenbearbeiter

[Rz 25] Die Empfehlungen der International Working Group on Data Protection in Telecommunications (IWGDPT)[43] nehmen den jeweiligen Datenbearbeiter in die Pflicht. Danach ist dieser am besten in der Lage, den Einzelfall in seiner Gesamtheit zu beurteilen und muss entscheiden, ob die bearbeiteten Daten anonymisiert, pseudonymisiert oder bestimmbar bzw. re-identifizierbar sind. Ferner wird vorgesehen, dass für den Fall einer Anonymisierung unter anderem eine Datenschutzfolgeabschätzung durchgeführt und die Verlässlichkeit der Anonymisierungstechnik geprüft werden muss. Im Ergebnis könnte also der Big-Data-Bearbeiter selber entscheiden, ob seine Bearbeitung unter das DSG fällt oder nicht. Angesichts des immer möglichen potentiellen Personenbezugs ist auch dieser Ansatz nicht optimal.

4.4.4 Zwischenfazit

[Rz 26] Zusammenfassend kann festgehalten werden, dass die technischen Möglichkeiten es zunehmend erlauben, die gigantische Menge der beschafften Daten ohne übermässigen Aufwand im Einzelfall zu re-identifizieren und damit einen Personenbezug herzustellen, sofern es sich nicht ohnehin bereits um Personendaten handelt. Infolgedessen dürfte die Anwendung der Datenschutzgesetzgebung vermehrt bejaht werden können. Damit entpuppt sich der grosse technische bzw. wirtschaftliche Vorteil von Big Data — mindestens aus datenschutzrechtlicher Sicht — als Nachteil bzw. Eingriff in die Persönlichkeitsrechte und zieht zahlreiche Rechte und Pflichten nach sich.

5 Erkennbarkeit der Datenbeschaffung und Zweckbindung

5.1 Ausgangslage und Problematik

[Rz 27] Die Beschaffung von Personendaten, insbesondere der Zweck ihrer Bearbeitung sowie jeder weitere Schritt der Datenbearbeitung[44] müssen für die betroffene Person erkennbar sein (Art. 4 Abs. 4 DSG). Die Erkennbarkeit ist bezüglich der wesentlichen Rahmenbedingungen der Datenbearbeitung sicherzustellen[45]. Auf diese Weise soll Transparenz geschaffen werden, damit die betroffene Person die Möglichkeit erhält, zu entscheiden, ob sie sich einer Datenbearbeitung grundsätzlich widersetzen[46] oder diese akzeptieren will.

[Rz 28] Dies ist im Rahmen von Big Data oft problematisch: In der Regel sind die Ergebnisse

42 BGE 136 II 508 S. 515, Erw. 3.4.

43 Working Paper, a.a.O., S. 13.

44 Maurer-Lambrou/Steiner, in: Maurer-Lambrou/Vogt, Basler Kommentar, 2014, Art. 4 DSG, Rz. 8.

45 Lucien Müller, Videoüberwachung in öffentlich zugänglichen Räumen: insbesondere zur Verhütung und Ahndung von Straftaten, Diss., Zürich/St. Gallen, 2011, S. 83.

46 Rosenthal, a.a.O., Art. 4, N 51.

einer Datenbearbeitung oder deren künftige Zwecke sowie deren Bekanntgabe an weitere Datenbearbeiter im Zeitpunkt der Beschaffung unklar. Ferner vermögen die betroffenen Personen die Bearbeitung von Daten aus unterschiedlichen Quellen kaum zu überblicken und nachzuvollziehen[47].

5.2 Lösungsansätze

[Rz 29] Beim Grundsatz der Erkennbarkeit ist der Spielraum, wenn überhaupt, sehr gering: Big-Data-Bearbeiter müssen eine klare sowie verständliche Mitteilung samt Offenlegung der bearbeiteten Daten, des Bearbeitungszwecks und einer Bekanntgabe an Dritte sowie Informationen zu den verwendeten Algorithmen sicherstellen[48]. Denkbar wäre die Verwendung von (am besten international standardisierten) Piktogrammen[49], welche den betroffenen Personen eine einfache und sprachenunabhängige Übersicht über die Datenbearbeitung verschaffen würden.

6 Zweckbindung

6.1 Ausgangslage und Problematik

[Rz 30] Gemäss Art. 4 Abs. 3 DSG dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Konkret bedeutet dies folgendes: Für die betroffene Person muss im Zeitpunkt der Datenbeschaffung klar und erkennbar sein, dass und für welche Zwecke ihre Daten bearbeitet werden. Ferner dürfen die so beschafften Personendaten nicht zweckentfremdet werden, d.h. ist ein Zweck (verstanden als Ziel einer Handlung[50]) für die Bearbeitung der Personendaten bei der Beschaffung einmal «gesetzt», so ist dieser auch bei einer späteren Bearbeitung grundsätzlich einzuhalten[51]. Damit geht eine gewollte Einschränkung der Datenbearbeitung einher, welche eine (unkontrollierte) Datenbekanntgabe zu Lasten der Persönlichkeitsrechte der betroffenen Person verhindern soll[52].

[Rz 31] Im Rahmen von Big Data werden Daten oft mehrfach und verschiedenen Datenbearbeitern bekanntgegeben[53], diese wiederum bearbeiten die erhaltenen Daten für andere Zwecke als die ursprünglichen Datenbearbeiter: Personendaten werden bspw. auf Social-Media-Portalen gesammelt und mittels Big Data Technologien in Nutzerprofile gewandelt (sog. Profiling). Durch die Zusammenführung vieler Einzeldaten wird es möglich, über die Einzelinformationen hinaus weitere Informationen zu gewinnen. Z.B. kann so das Kaufverhalten erkannt und zu Marketingzwecken an weitere Datenbearbeiter (z.B. Werbeagenturen) weitergegeben und kommerzialisiert werden[54].

---

47 EDÖB, Erläuterungen zu Big Data, a.a.O.

48 Resolution of Big Data, p.2.

49 Lucien Müller, a.a.O., S. 86.

50 http://www.duden.de/rechtschreibung/Zweck.

51 Lucien Müller, a.a.O., S. 79.

52 Lucien Müller, a.a.O., S. 78.

53 Resolution of Big Data, p. 1.

54 Rolf H. Weber/Dominic N. Staiger, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz —

[Rz 32] Anlässlich der erstmaligen Beschaffung und Bearbeitung der Daten (beim Profiling; vgl. oben) mag der Grundsatz der Zweckbindung noch eingehalten werden. Jedoch spätestens bei der Weitergabe zur Bearbeitung zu anderen Zwecken (Auswertung des Kaufverhaltens und Veräusserung an Dritte etc.) können sich Schwierigkeiten ergeben. Wurden diese neuen bzw. anderen Zwecke nicht bei der Beschaffung angegeben und waren sie auch nicht aus den Umständen ersichtlich oder gesetzlich vorgesehen, wäre der Grundsatz der Zweckbindung nicht eingehalten.

[Rz 33] Die Angabe eines sehr weit gefassten Zwecks vermag diese Schwierigkeit nicht zu lösen. Die Zweckbindung kann ihre Funktion nur dann erfüllen, wenn der Zweck hinreichend detailliert ist, damit beurteilt werden kann, ob die Datenbearbeitung im Einzelfall davon abgedeckt ist oder nicht[55]. Erschwerend kommt hinzu, dass oftmals bei der Beschaffung gar nicht klar ist, wer die fraglichen Daten wie, wann und letztlich zu welchem Zweck bearbeitet.

[Rz 34] Aufgrund der nicht transparenten Big-Data-Bearbeitungen und -Bearbeiter ist davon auszugehen, dass sich sämtliche tatsächlichen Bearbeitungszwecke nicht aus dem Umstand und auch nicht aus dem Gesetz ergeben. Damit würde eine Verletzung der Persönlichkeitsrechte der betroffenen Person vorliegen, die gemäss Art. 12 f. DSG durch überwiegende private oder öffentliche Interessen oder durch die Einwilligung der betroffenen Person gerechtfertigt werden könnte (s. Ziff. 7 hienach).

6.2 Lösungsansätze

[Rz 35] Thouvenin verweist in diesem Zusammenhang auf die Entstehungsgeschichte des DSG, wonach ursprünglich zwei Vorentwürfe vorgelegen seien: einer für den öffentlich-rechtlichen und einer für den privatrechtlichen Bereich. Dabei sei der Grundsatz der Zweckbindung im heutigen Sinn anfänglich nur im Vorentwurf für den öffentlich-rechtlichen Bereich (d.h. für die Bundesverwaltung) und nicht für den Privatbereich vorgesehen gewesen. Ferner sei nicht davon auszugehen, dass die Zweckbindung zum Schutz der Privatsphäre der betroffenen Personen «*sondern vielmehr als logische Folge der Beschränkung des staatlichen Handelns in einem grundrechtlich geschützten Bereich, mithin eine Konkretisierung der Voraussetzungen der gesetzlichen Grundlage, des öffentlichen Interesses und des Verhältnismässigkeitsprinzips zu verstehen sei*». Thouvenin stellt in diesem Zusammenhang u.a. die Frage, ob das Zweckbindungsprinzip im Privatbereich einen grösseren Spielraum erhalten oder die Einwilligung grosszügiger und inhaltlich weiter gefasst werden solle[56].

[Rz 36] Etwas weniger grosszügig sind die meisten Datenschutzbehörden der europäischen Staaten: Sie plädieren für eine strikte Einhaltung des Grundsatzes der Zweckbindung[57].

[Rz 37] Denkbar und in Übereinstimmung mit den Empfehlungen[58] der IWGDPT wäre folgende Lösung: Für den Fall, dass der Datenbearbeiter bereits beschaffte Personendaten zu einem neuen Zweck bearbeiten möchte, müsste im Einzelfall eine Prüfung der Kompatibilität des bisherigen

Gegenseitige Herausforderungen, Zürich 2014, S. S. 158.

55 Weichert, a.a.O., S. 13.

56 Aurelia Tamo, Veranstaltung des Zentrums für Informations-und Kommunikationsrecht der Universität Zürich, der Forschungsstelle für Informationsrecht der Universität St. Gallen und des Schweizer Forum für Kommunikationsrecht SFFS vom 31. Oktober 2013, in: sic! 5|2014, 331, S. 4f.

57 Resolution of Big Data, p. 2.

58 Working Paper, a.a.O., S. 13.

sowie des neuen Zwecks durchgeführt werden. Dabei müssten insbesondere folgende Schlüsselelemente beurteilt werden: (i) Verhältnis zwischen dem alten und dem neuen Bearbeitungszweck, (ii) der Umstand der Beschaffung der bisherigen Daten und die vernünftige Erwartung der betroffenen Person bezüglich der künftigen Bearbeitung dieser Daten, (iii) die Natur der beschafften Daten und die Konsequenz der neuen Bearbeitung auf die betroffenen Personen, (iv) Schutzmassnahmen der Datenbearbeiter zur Sicherstellung einer fairen Datenbearbeitung und zur Verhinderung derer ungebührlicher Auswirkungen auf die betroffenen Personen. Diese Aspekte könnten m.E. im Rahmen der Rechtfertigungsgründe gemäss Art. 13 DSG berücksichtigt werden und in die Interessenabwägung einfliessen.

7 Verhältnismässigkeit

7.1 Ausgangslage und Problematik

[Rz 38] Art. 4 Abs. 2 DSG sieht die Verhältnismässigkeit als Grundsatz für jede Datenbearbeitung vor. Konkret bedeutet dies folgendes: Erstens hat sowohl der Zweck wie auch die Art und Weise der Datenbearbeitung selbst verhältnismässig zu sein. Dies setzt voraus, dass die Datenbearbeitung überhaupt zu einem klaren, im Voraus festgelegten Zweck erfolgt. Zweitens, dürfen nur diejenigen Daten bearbeitet werden, die geeignet sind, um den festgelegten Zweck zu erreichen (Eignung). Drittens hat der Datenbearbeiter danach zu fragen, ob der Zweck der Datenbearbeitung auch mit der Bearbeitung von weniger bzw. weniger einschneidenden Daten (bspw. ohne besonders schützenswerten Personendaten[59] oder Persönlichkeitsprofilen[60]) erreicht werden kann (Erforderlichkeit). Dies setzt voraus, dass der Zweck der Datenbearbeitung bekannt ist, und nur genau so viele Daten bearbeitet werden, wie absolut nötig, damit die Datenbearbeitung überhaupt Sinn macht. Nachdem der vorgesehene Zweck erreicht ist, müssen zudem sämtliche nicht mehr benötigten Daten gelöscht und dürfen nicht mehr wiederverwendet werden. Nicht verhältnismässig ist eine Datenbearbeitung auf Vorrat ohne konkreten Verwendungszweck (d.h. ein «Sammeln» für den Fall, dass man die Daten später vielleicht brauchen könnte). Viertens darf die Datenbearbeitung nicht in einem Missverhältnis zum angestrebten Zweck stehen (Zumutbarkeit). Schliesslich müssen die vorgenannten Kriterien für jeden Einzelfall gesondert geprüft werden; jede Datenbearbeitung muss verhältnismässig sein (dient die Datenbearbeitung mehreren Zwecken, hat sie für jeden einzelnen Zweck verhältnismässig zu erfolgen)[61].

[Rz 39] Verhältnismässigkeit im vorgenannten Sinne widerspricht dem Konzept von Big Data grundlegend: «*Big Data is about data maximisation. In essence, Big Data is the very antithesis of the privacy principles of relevance and data minimisation*»[62]. Der gigantische und ständig zunehmende Umfang an Daten (das weltweite Datenvolumen wächst 50% pro Jahr[63]) über beliebig viele Themen sind wichtiges Wesensmerkmal und zugleich grosser Vorteil von Big Data. Dabei kommt der potentiellen, künftigen Nutzung der Daten eine grosse Bedeutung zu[64]. Danach könnten Daten,

[59] Art. 3 lit. c DSG.

[60] Art. 3 lit. d DSG.

[61] Rosenthal, a.a.O., Art. 4 Abs. 2, N 20 ff.

[62] Working Paper, a.a.O., S. 6.

[63] Working Paper, a.a.O., S. 2.

[64] Working Paper, a.a.O., S. 6.

die heute nicht wichtig oder nicht mehr benötigt erscheinen, morgen einen Mehrwert erbringen. Nur wer möglichst viele Daten aus den verschiedensten Quellen für möglichst lange Zeit und zu potentiell neuen Zwecken bearbeitet, kann daraus den maximalen Nutzen ziehen.

[Rz 40] Dies hat Konsequenzen: Werden Personendaten auf diese unverhältnismässige Weise von Big Data Technologien bearbeitet, liegt eine Persönlichkeitsrechtsverletzung vor (eine allfällige Rechtfertigung gemäss Art. 13 DSG wäre jedoch denkbar; vgl. Ziff. 7.2 und 8 hienach).

7.2 Lösungsansätze

[Rz 41] Wenn man sich die anfangs genannten Wesensmerkmale von Big Data erneut vor Augen führt, wird ohne Weiteres ersichtlich, dass die verwendeten Big Data Technologien und der datenschutzrechtliche Bearbeitungsgrundsatz der Verhältnismässigkeit auf Kriegsfuss stehen. Aus datenschutzrechtlicher Sicht führt dies zu grossen Herausforderungen und eine griffige Lösung scheint dabei schwierig: Big-Data-Bearbeiter müssten zur Einhaltung der Verhältnismässigkeit sensibilisiert[65]und motiviert werden. Eine datenschutzrelevante Datenbearbeitung muss grundsätzlich verhältnismässig erfolgen[66]. Das Sammeln auf Vorrat für nicht feststehende Zwecke ist in jedem Fall zu verneinen[67]. Alsdann dürften Big-Data-Bearbeiter die Möglichkeiten der Rechtfertigung gemäss Art. 13 Abs. 1 DSG, insbesondere auf dem Wege einer gültigen Einwilligung, regelmässig ausschöpfen und damit etwas Spielraum für die benötigte Datenbearbeitung erhalten (vgl. Ziff. 8 hienach). Dies gilt jedoch nur für den Privatbereich; Bundesorgane müssen ihre Daten immer verhältnismässig bearbeiten und sich an Art. 5 Abs. 2 BV i.V.m. Art. 13 Abs. 2 BV halten.

8 Einwilligung

8.1 Ausgangslage und Problematik

[Rz 42] Die Bearbeitung von Personendaten setzt grundsätzlich keine Einwilligung der betroffenen Person voraus. Die Einwilligung gemäss Art. 4 Abs. 5 DSG ist Ausfluss der informationellen Selbstbestimmung der betroffenen Person. Letztere kann den Bearbeitungsgrundsätzen des DSG widersprechen[68] und auf einen standardmässig vorgesehen Schutz verzichten: Bspw. kann sich die betroffene Person auf die Bekanntgabe ihrer Personendaten in ein Land ohne angemessene Datenschutzgesetzgebung einverstanden erklären (Art. 6 Abs. 2 lit. b DSG). Sie kann z.B. auch eine Datenbearbeitung zu anderen als den bei der Beschaffung angegebenen Zwecken oder in einem grösseren (unverhältnismässigen) Umfang akzeptieren (Art. 13. Abs. 1 DSG). Denkbar ist auch die Einwilligung in eine Datenbearbeitung durch Bundesorgane ohne eine gesetzliche Grundlage (Art. 17 Abs. 2 lit. c und Art. 19 Abs. 1 lit. b DSG).

[Rz 43] Die Einwilligung gemäss Art. 4 Abs. 5 DSG ist gültig, wenn die betroffene Person rechtzeitig über die Datenbearbeitung angemessen informiert wurde und freiwillig einwilligt. Für die

65 Working Paper, a.a.O., S. 17.

66 Rolf H. Weber, Big Data: Rechtliche Perspektive, a.a.O., S. 26.

67 Rosenthal, a.a.O., Art. 4 Abs. 3, N 31.

68 Rosenthal, a.a.O., Art. 4 Abs. 5, N 67.

Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen (Art. 4 Abs. 5 Satz 2 DSG). Die Voraussetzung der angemessenen Information ist dann erfüllt, wenn die betroffene Person zumindest in groben Zügen wissen kann, welche Art von Daten von wem und zu welchem Zweck bearbeitet werden[69]. Mit anderen Worten müssen Ausmass und Inhalt der Datenbearbeitung für die betroffene Person abschätzbar sein. Ferner muss die Einwilligung verweigert oder nachträglich widerrufen werden können. Sie kann schriftlich oder mündlich erfolgen und ist an keine bestimmte Form gebunden. Ungenügend sind Pauschalermächtigungen[70], womit in sämtliche möglichen Datenbearbeitungen eingewilligt wird; diese schaffen keine genügende Transparenz[71].

[Rz 44] Beispielsweise im Online-Verkehr ist schon heute oft fraglich, ob die Voraussetzungen für eine gültige Einwilligung vollständig erfüllt werden. Die jeweiligen Datenschutzerklärungen von Unternehmen sind oft nicht ausreichend klar und unvorteilhaft dargestellt; die Datenbearbeitung ist kaum abschätzbar. Zudem ist unklar, ob ein blosser «Klick» zur Abgabe einer Einwilligung ausreicht, insbesondere dann, wenn die umfangreiche Datenschutzerklärung nicht gelesen, geschweige denn verstanden wurde (bspw. umfasst die Datenschutzerklärung von Google Schweiz zehn Seiten mit weiterführenden Links). Problematisch ist auch die Einwilligung durch das «Anklicken» von online AGB: Auf diesem Wege wird die betroffene Person in der Regel keine gültige Einwilligung abgeben können[72].

[Rz 45] Dieses Problem wird bei Big Data nochmals akzentuiert, insbesondere wenn der Umfang und/oder Zweck der Datenbearbeitung, zu welcher die betroffene Person ihre Einwilligung (gültig) abgegeben hat, nachträglich erweitert wird: Werden Daten bearbeitet, um einem beliebigen Zweck in der Zukunft zu dienen, kann wohl nicht einmal der erste Big-Data-Bearbeiter Ausmass und Inhalt der Datenbearbeitung abschätzen, geschweige denn die betroffene Person; aufgrund der theoretisch unbegrenzten Möglichkeiten der Datenbearbeitung wird sie wohl kaum jemals eine angemessene Abschätzung durchführen können. Auch wenn hinsichtlich des jeweils weiteren bzw. neuen Bearbeitungszwecks Klarheit bestünde, wäre das Einholen zahlreicher Einwilligungen bei jeder betroffenen Person schon aus praktischen Gründen problematisch[73].

8.2 Lösungsansätze

[Rz 46] Als möglicher Ausweg wäre eine detaillierte und klare vertragliche Regelung der vorgesehenen Datenbearbeitung denkbar. Diese Lösung muss aber angesichts der fehlenden Praktikabilität sowie des offenbar nicht vorhandenen Bedürfnisses der betroffenen Personen verworfen werden[74]: trotz möglicher negativer Konsequenzen wollen sich erfahrungsgemäss nur wenige Personen Zeit nehmen, um für «Alltägliches» Verträge samt «Kleingedruckten» zu prüfen und abzuschliessen.

---

69 Rosenthal, a.a.O., Art. 4 Abs. 5, N 72.

70 EDÖB, Erläuterungen zu Big Data, a.a.O.

71 Astrid Epiney, Datenschutzrecht in der Schweiz. Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Freiburger Schriften zum Europarecht Nr. 10, 79 S., Freiburg 2009, S. 42.

72 Rolf H. Weber, Big Data, Sprengkörper des Datenschutzrechts?, in: Jusletter IT 11. Dezember 2013, S. 5 f.

73 Thilo Weichert, a.a.O., S. 13.

74 Rolf H. Weber, Big Data: Rechtliche Perspektive, a.a.O., S. 26.

[Rz 47] Denkbar wäre auch die Argumentation mit dem sog. Vertrauensverhältnis zwischen Datenbearbeiter und der betroffenen Person im Rahmen einer längeren Geschäftsverbindung, wonach eine Einwilligung in bspw. eine Datenbearbeitung zu einem neuen Zweck durch Stillschweigen vorliegen könnte[75]. Ein solches Vertrauensverhältnis dürfte jedoch in den seltensten Fällen vorliegen, da bei Big Data gerade nicht klar ist, wer welche Daten wann bearbeitet.

9 Ausblick

9.1 Digitales Grundrecht

[Rz 48] Die Einführung eines «*digitalen Grundrechts*», wonach sämtliche Personendaten im Eigentum der betroffenen Person stehen, wurde diskutiert: Anfang 2015 sprach sich die staatspolitische Kommission des Nationalrates (SPK-N) mit 13 zu 9 Stimmen bei 1 Enthaltung für die parlamentarische Initiative «*Schutz der digitalen Identität von Bürgerinnen und Bürgern*» von NR Fathi Derder (FDP/VD) aus. Danach soll Art. 13 Abs. 2 BV wie folgt umformuliert werden: «*Die Daten sind Eigentum der betreffenden Person; diese ist davor zu schützen, dass die Daten missbräuchlich verwendet werden*». Der Initiant verspricht sich durch eine Verankerung in der Bundesverfassung, einen besseren Schutz der Personendaten vor Missbrauch[76]. Dieser Vorstoss wurde bisher noch nicht in den eidgenössischen Räten behandelt. Seine allfällige Umsetzung ist daher ungewiss; er könnte jedoch einen Einfluss auf die Datenschutzgesetzgebung haben und diese allenfalls in ihrem Anwendungsbereich ausweiten. Im Ergebnis wäre denkbar, dass hieraus Bearbeitungsgrundsätze resultieren könnten, welche auf Big Data Anwendung finden würden.

9.2 Privacy by design und Accountability

[Rz 49] Gemäss Empfehlung der IWGDPT sollen Big Data Technologien einerseits auf dem «privacy by design»-Grundsatz beruhen[77]. Danach würden datenschutzrechtliche Aspekte bereits von Anfang an bei Big Data Technologien einbezogen um so frühzeitig deren rechtskonforme Entwicklung und Anwendung sicherzustellen[78]. Konkret könnten bspw. bei der Gestaltung von Big Data Technologien Quelldaten und für Analysezwecke verwendete Daten strikt getrennt werden, während die eigentliche Verknüpfung und Analyse ausschliesslich mit stark pseudonymisierten und anonymisierten Daten erfolgen würde. Im Falle einer Bekanntgabe an Ditte, müsste zudem sichergestellt werden, dass diese auch mit «Zusatzwissen» keine Re-Identifizierung vornehmen könnten[79].

[Rz 50] Andererseits soll das Accountability-Prinzip («Rechenschaft ablegen», d.h. Offenlegung und Einhaltung der angewendeten Datenbearbeitungen) sicherstellen, dass der Datenbearbei-

---

75 Rosenthal, a.a.O., Art. 4 Abs. 5, N 81.

76 Michal Cichocki, Staatspolitische Kommission des Nationalrates will Personendaten besser vor Missbrauch schützen, 16. Januar 2015, http://www.lawblogswitzerland.ch/2015/01/staatspolitische-kommission-des.html.

77 1. Proactive not Reactive; Preventative not Remedial, 2. Privacy as the Default Setting, 3. Privacy Embedded into Design, 4. Full Functionality — Positive-Sum, not Zero-Sum, 5. End-to-End Security — Full Lifecycle Protection, 6. Visibility and Transparency — Keep it Open, 7. Respect for User Privacy — Keep it User-Centric; Working Paper, a.a.O., S. 16.

78 EDÖB, Erläuterungen zu Big Data, a.a.O.

79 Cavoukian A./ Jonas J., Privacy by design in the age of big data, 2012.

ter sich der potentiellen datenschutzrechtlichen Gefahren von Big Data (z.B. Re-Identifizierung, Zweckbindung etc.) bewusst ist und die verwendeten Big Data Technologien unter diesen Aspekten fortwährend überprüft[80].

9.3 Sektorspezifische Regulierung

[Rz 51] Parallel zu allenfalls neuen, Big-Data-spezifischen Bestimmungen im Rahmen der laufenden DSG-Revision oder der künftigen Datenschutzgrundverordnung in der EU, wäre eine sektorspezifische Regulierung von Big Data für Branchen mit besonders sensiblen Daten denkbar: Bspw. könnte im e-Health[81] Bereich eine auf Big Data zugeschnittene Regulierung diskutiert werden[82]. Um der Dynamik von Big Data hinreichend Rechnung tragen zu können, würde sich das Rechtskleid eines Soft-Law-Regelwerks durch Branchenverbände anbieten (bspw. analog Verhaltensrichtlinien der schweizerischen Telekommunikationsunternehmen zur Netzneutralität)[83]. Dies würde zwar nur, aber immerhin, nicht-bindende, dafür umso flexiblere Rahmenbedingungen für den Einsatz von Big Data abstecken.

10 Fazit

[Rz 52] Big Data und Datenschutz müssen nicht (zwangsweise) im Widerspruch stehen. Im Idealfall könnte der potentiellen Möglichkeit einer Re-Identifizierung aufgrund der zunehmenden Datenmenge frühzeitig, d.h. ab Beschaffung und bereits vor Vorliegen von Personendaten, durch die Beachtung der datenschutzrechtlichen Bearbeitungsgrundsätze Rechnung getragen werden. Falls dies nicht möglich sein sollte, würde mindestens eine transparente Offenlegung der Bearbeitungsmethoden sowie deren Zwecke — für jeden und jeden neuen Bearbeitungszweck — und die Bearbeitung nur derjeniger Daten, die für die Zweckerreichung der Datenbearbeitung nötig sind, ebenfalls latentes Konfliktpotential entschärfen.

Michal Cichocki, MLaw, ist Rechtsanwalt sowie stellvertretender Datenschutz- und Informationsschutzverantwortlicher im Rechtsdienst/Datenschutz im Stab im Bundesamt für Polizei (fedpol). Der vorliegende Aufsatz gibt ausschliesslich die persönliche Auffassung des Autors wieder.

---

80 Working Paper, a.a.O., S. 17.

81 «Elektronische Dienste im Gesundheitswesen»; mit elektronischen Mitteln werden im Gesundheitswesen Abläufe digitalisiert und Patienten, Ärzte, Versicherte, Versicherungen, Labors, Apotheken, Spitäler etc. vernetzt.

82 Rolf H. Weber, Big Data, Sprengkörper des Datenschutzrechts?, in: Jusletter IT 11. Dezember 2013, S. 8.

83 Michal Cichocki, Netzneutralität: schweizerische Telekommunikationsunternehmen arbeiten Verhaltensrichtlinien aus, 9. November 2014, http://www.lawblogswitzerland.ch/2014/11/netzneutralitat-schweizerische.html.