www.jusletter-it.eu

Astrid Epiney

Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?

In the course of technical development «Big Data» enables the analytic linking of large amounts of data that could also concern identifiable persons. The article shows the data protection regulations that must be observed in this regard (with a focus on the question of the applicability of the data protection laws) and on this basis throws up the question whether legislative action is needed. (ah)

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

Citation: Astrid Epiney, Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?, in: Jusletter IT 21 May 2015

Inhaltsübersicht

I. Einleitung

[Rz 1] Das Phänomen «*Big Data*» ist in den letzten Jahren vermehrt in den Fokus nicht nur der (rechts-)wissenschaftlichen Diskussion, sondern auch einer breiteren Öffentlichkeit gelangt. Dies dürfte in erster Linie mit den beachtlichen technischen Entwicklungen im Bereich der Datenbearbeitung und der Datenverknüpfung sowie dem bedeutenden wirtschaftlichen Potenzial zusammenhängen.[1] Mit dem Begriff «*Big Data*» — wobei sich seine Konturen durchaus nicht durch ein Übermass an Klarheit auszeichnen bzw. er eine Vielfalt von Tätigkeiten umfasst[2] — wird üblicherweise eine (festzulegende analytische) Verknüpfung einer Reihe von (stetig steigenden) verfügbaren Daten (wobei es sich nicht zwingend um Personendaten im Sinne von Art. 3 lit. a DSG handelt) bezeichnet. Diese Verknüpfung erfolgt unter Rückgriff auf hierfür geeignete und in der Regel auch zu diesem Zweck entwickelte informationstechnologische Verfahren. Ziel ist die Gewinnung zusätzlicher Erkenntnisse, die wirtschaftlicher, politischer, wissenschaftlicher oder sozialer Natur sein können.

[Rz 2] Folgende Beispiele mögen dies illustrieren:

- Durch *Big Data* sollen etwa Manipulationen im Börsenhandel leichter erkennbar werden.
- Auch verspricht man sich, ATPs (*Advanced Persistent Threat*) wirksamer begegnen zu können. *Big Data* räumt etwa die Möglichkeit ein, ATPs aufgrund eines Abgleichs des bisherigen Nutzungsverhaltens zu ermitteln.[3]
- Auch im Gesundheitsbereich kann *Big Data* zum Einsatz kommen: So werden z.B. in Entwicklungsländern Röntgenbilder, die in kleineren Spitälern erhoben werden, an grössere geschickt, um sie zu diagnostizieren. *Big Data* ermöglicht es sodann, diese Vielzahl von Rönt-

[1] Zur wirtschaftlichen Bedeutung etwa Bruno Baeriswyl, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz — Gegenseitige Herausforderungen, Zürich 2014, 46.

[2] S. auch noch sogleich unten II.

[3] Andreas Wespi, Big Data: Technische Perspektive, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz — Gegenseitige Herausforderungen, Zürich 2014, 3 (10 ff.), Florent Thouvenin, Grundprinzipien des Datenschutzrechts auf dem Prüfstand, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz — Gegenseitige Herausforderungen, Zürich 2014, 62 (63).

genbildern anhand von Merkmalen zu kategorisieren. Bilder gleicher Kategorie werden dann jeweils den gleichen Experten vorgelegt.[4]
- Der Einsatz im Marketing erlaubt die grossflächige Analyse des Marktverhaltens der Konsumenten und damit eine sehr zielgerichtete Werbung.
- Im Verkehrsbereich können möglicherweise Gefahrenpotentiale besser identifiziert werden, so z.B. durch die Analyse des Fahrverhaltens in Anknüpfung an Standortdaten.
- Grosses Potential besteht in der Wissenschaft, die für ihre Analysen auf fast unbegrenzte Datenmengen zurückgreifen kann.

[Rz 3] Soweit im Rahmen von *Big Data* personenbezogene Daten bearbeitet werden, liegt das Risikopotential für die Persönlichkeitsrechte der Betroffenen auf der Hand, erlaubt es die Verknüpfung von Daten und ihre Analyse im Rahmen von *Big Data* doch, umfassende Informationen über die Betroffenen zu erlangen, womit in der Regel auch eigentliche Persönlichkeitsprofile einhergehen werden. Deutlich wird damit das bedeutende Macht- und Missbrauchspotential der durch *Big Data* ermöglichten Analysen, womit elementare grundrechtliche Gewährleistungen betroffen sind bzw. sein könnten. Diese Gefahren können sich auch im Zuge der Bearbeitung von zunächst anonymisiert erscheinenden Daten, die im Zuge des Einsatzes von *Big Data* re-identifiziert werden, realisieren.

[Rz 4] Aufgeworfen wird damit die Frage, ob ein gesetzgeberischer Handlungsbedarf insofern besteht, als die Vorgaben des Datenschutzrechts (sei es auf kantonaler, nationaler oder europäischer Ebene) an die skizzierten, mit *Big Data* einhergehenden, zumindest teilweise durchaus neuen Herausforderungen angepasst bzw. ergänzt werden müssten oder sollten. Die nachfolgenden Überlegungen sollen einen Beitrag zur Behandlung dieser Problematik leisten, wobei schon an dieser Stelle bemerkt sei, dass es nicht um eine vollständige Erörterung der angesichts der Vielschichtigkeit schon des Begriffs *Big Data* sehr komplexen und facettenreichen Thematik gehen kann. Vielmehr soll — ausgehend von einer Annäherung an den Begriff (II.) — nur (aber immerhin) aufgezeigt werden, welche datenschutzrechtlichen Vorgaben im Zusammenhang mit *Big Data* unter welchen Voraussetzungen von besonderer Bedeutung sind (III.), um in einer kurzen Schlussbemerkung (IV.) eine notwendigerweise vorläufige Antwort auf die Frage nach dem gesetzgeberischen Handlungsbedarf zu geben.

II. Big Data — Zum Begriff

[Rz 5] Üblicherweise wird unter dem Begriff *Big Data* die unter Rückgriff auf Informationstechnologien und damit in der Regel sehr schnell erfolgende Analyse ausgesprochen grosser («*big*») Datenmengen («*data*») bezeichnet, dies mit dem Ziel der Gewinnung entscheidungsrelevanter (in welchem Bereich auch immer) Erkenntnisse, möglicherweise — je nach Nutzungsbereich — gar in sog. Echtzeit.[5]

---

4 Wespi, in: Big Data (Fn. 3), 3 (8).

5 Vgl. im Einzelnen BITKOM, Big Data im Praxiseinsatz — Szenarien, Beispiele, Effekte, 2012, 7 ff., verfügbar unter www.bitkom.org/de/publikationen/38337_73446.aspx; www.webopedia.com/TERM/B/big_data.html (alle Internetquellen zuletzt abgerufen am 18. Februar 2015). Zum Begriff auch Wespi, in: Big Data (Fn. 3), 3; Mario Martini, Big Data als Herausfordeurng für den Persönlichkeitsschutz und das Datenschutzrecht, DVBl. 2014, 1481 (1482 f.), wobei letzterer als Beispiele hauptsächlich die Bearbeitung personenbezogener Daten im Rahmen von *Big Data* erwähnt.

[Rz 6] Deutlich wird damit auch, dass es sich bei *Big Data* gerade nicht — wie die grammatikalische Form bzw. der Begriff suggerieren könnte — nur um eine (feststehende) «Datenmenge» handelt, sondern dass es auch um Tätigkeiten (das Analysieren und Verwerten grosser Datenmengen durch eine leistungsfähige IT-Infrastruktur und auf der Grundlage definierter Algorithmen) geht. M.a.W. nimmt der Begriff *Big Data* offenbar einerseits Bezug auf eine Tätigkeit (das Analysieren), andererseits aber auch auf das Ergebnis dieser Tätigkeit (das Analyseresultat) und damit die gewonnen Daten. Somit lässt sich der Begriff *Big Data* in mindestens drei Bestandteile gliedern:[6]

- die Menge an Daten aus einer Vielzahl von Quellen, wodurch die Datenmenge sowie die Datenart letztlich im Grundsatz unbegrenzt sind;
- der gesamte Prozess von der Beschaffung der Daten, über die Einordnung und Analyse dieser Daten zum Zweck der Informationsgewinnung bis hin zu ihrer Verwertung (auch *Big Data Analytics* genannt);[7]
- der Rückgriff auf spezielle Softwarewerkzeuge,[8] die auch eine Echtzeit-Analyse erlauben.

[Rz 7] Deutlich wird damit auch, dass *Big Data* letztlich eine besonders weitgehende Form der Datenverknüpfung darstellt: Als eine solche wird das «Zusammenführen von Daten aus ein oder mehreren Datenquellen» bezeichnet,[9] ein Merkmal, das nach dem Gesagten auch bei *Big Data* gegeben ist, wobei sich die Datenverknüpfung bei *Big Data* durch die Unbegrenztheit der verknüpften Daten sowie den Rückgriff auf Informationstechnologien auszeichnet.

[Rz 8] Dabei kann sich *Big Data* sowohl auf personenbezogene als auch auf nicht personenbezogene Daten beziehen; nur im erst genannten Fall stellen sich datenschutz- und persönlichkeitsrechtsrelevante Fragen aufgrund der Anwendbarkeit des Bundesgesetzes über den Datenschutz (DSG) oder der kantonales Datenschutzgesetze, womit dieser Aspekt im vorliegenden Zusammenhang von besonderer Bedeutung sein dürfte.[10]

III. Big Data und Datenschutzrecht de lege lata

[Rz 9] Es versteht sich von selbst, dass das Datenschutzrecht — wie die gesamte Rechtsordnung — auch für die Datenbearbeitungen im Rahmen von *Big Data* massgeblich ist. Allerdings muss der Anwendungsbereich des Datenschutzgesetzes eröffnet sein (1.), bevor auf ausgewählte datenschutzrechtliche Grundsätze in diesem Zusammenhang hingewiesen werden soll (2.).

---

6 Darüber hinaus bzw. präzisierend wird Big Data auch oft über «Vs» beschrieben, wobei deren Anzahl variiert. Üblicherweise wird (mindestens) auf folgende «Vs» Bezug genommen: *volume*, *velocity*, *variety*, *veracity* und *value*. Vgl. z.B. www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=de; http://dataconomy.com/seven-vs-big-data/; Wespi, in: Big Data (Fn. 3), 3 (4 ff.); Jean-Pierre König, Suchmaschinen und Social Media, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz — Gegenseitige Herausforderungen, Zürich 2014, 31 f. Ein zusätzlicher Erkenntniswert im Hinblick auf die vorliegende Problemstellung scheint mit dieser Begrifflichkeit nicht verbunden zu sein.

7 Dieser Aspekt steht gar im Vordergrund für das Begriffsverständnis von *Big Data*. Dies erschliesst sich vor dem Hintergrund, dass die Analyse solcher Bestände gerade Sinn und Zweck des Vorgehens ist. Vgl. Baeriswyl, in: Big Data und Datenschutz (Fn. 1), 46; Thouvenin, in: Big Data und Datenschutz (Fn. 3), 62.

8 http://www.webopedia.com/TERM/B/big_data_analytics.html.

9 Thomas Probst, Die Verknüpfung von Personendaten und deren rechtliche Tragweite, in: Astrid Epiney/Thomas Probst/Nina Gammenthaler (Hrsg.), Datenverknüpfung: Problematik und rechtlicher Rahmen, Zürich 2011, 1 (20), mit weiteren sehr instruktiven Präzisierungen (20 ff.).

10 S. insoweit sogleich unten III.

[Rz 10] Die folgenden Ausführungen beziehen und beschränken sich auf das Datenschutzgesetz des Bundes, wobei sich die entsprechenden Überlegungen jedoch zumindest weitgehend auch auf das EU-Datenschutzrecht sowie die kantonalen Datenschutzgesetze übertragen lassen.

1. Die Eröffnung des Anwendungsbereichs des Datenschutzgesetzes: das Vorliegen von Personendaten

a) Grundsätze

[Rz 11] Das Datenschutzgesetz gilt von vornherein nur für das Bearbeiten — eine Bearbeitung im Sinne des Art. 3 lit. e DSG liegt bei *Big Data* unproblematisch vor — von Personendaten (Art. 2 Abs. 1 DSG). Unter diesen sind nach Art. 3 lit. a DSG alle Angaben zu verstehen, die sich auf eine bestimmte oder bestimmbare Person beziehen. Sie sind somit abzugrenzen von Sachdaten, die nicht in den Anwendungsbereich des DSG fallen.[11] Bestimmt sind Daten, wenn diese unmittelbar die Identifizierung der Person ermöglichen, wie beispielsweise Visitenkarten oder Pässe. Bestimmbar ist die Person hingegen, wenn die Daten zwar für sich allein keinen Rückschluss auf eine Person ermöglichen, jedoch durch Einbezug weiterer Daten (Datenverknüpfung) gleichwohl eine Identifikation erfolgen kann.[12] Ob eine Bestimmbarkeit in diesem Sinn vorliegt, kann nicht durch generell-abstrakte Kriterien festgelegt werden, sondern ist unter Berücksichtigung aller Umstände des Einzelfalls zu entscheiden. Daher ist danach zu fragen, welches Interesse der Datenbearbeiter oder auch ein Dritter (und damit jede Person, die Zugang zu den Daten haben könnte) an der Identifizierung haben kann; hier reicht zwar die rein theoretische Möglichkeit der Identifizierung nicht aus, wenn sie mit derart viel Aufwand verbunden ist, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, sie werde tatsächlich wahrgenommen. Allerdings kann das Interesse an einer Identifizierung je nach Umständen auch dazu führen, dass jemand den Aufwand auf sich nehmen könnte, insbesondere wenn die technischen Möglichkeiten berücksichtigt werden. Deutlich wird damit auch, dass die Bestimmbarkeit — neben dem möglichen Interesse des Datenbearbeiters an einer Identifizierung der Personen — massgeblich von Umfang und Art der zur Verfügung stehenden (sonstigen) Angaben sowie dem (finanziellen und zeitlichen) Aufwand abhängt, den eine Identifizierung voraussichtlich mit sich bringt. Diese Faktoren können sich im Laufe der Zeit durchaus verändern, so dass es *a priori* möglich erscheint, dass bestimmte Angaben heute (noch) keine Personendaten darstellen, morgen jedoch — aufgrund z.B. der technischen Entwicklung — als solche zu betrachten sind, weil die Verknüpfungsmöglichkeiten derart gestiegen sind, dass nunmehr eine Bestimmbarkeit anzunehmen ist.

[Rz 12] Im Falle der Anonymisierung entfällt der Personenbezug immer dann, wenn die Möglichkeit der Zuordnung zu bestimmten Personen endgültig weggefallen ist; kann die Anonymisierung wieder rückgängig gemacht werden, dürfte das Vorliegen von Personendaten wohl nach denselben allgemeinen Kriterien zu ermitteln sein wie bei der Frage nach der Bestimmbarkeit einer

[11] Bruno Baeriswyl, «Big Data» ohne Datenschutz-Leitplanken, digma 1/2013, 14 (15).

[12] Vgl. im Einzelnen zur Bestimmbarkeit neben den einschlägigen Kommentaren Eva Maria Belser/Hussein Noureddine, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011, §7, Rn. 39 ff. Aus der Rechtsprechung ausführlich z.B. BGE 138 II 346 E. 6.1 («Google Street View»); BGE 136 II 508 E. 3 («Logistep»). Ausführlich und sehr instruktiv Thomas Probst, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Person im Datenschutzrecht, Personendaten und anonymisierte Einzeldaten in der globalisierten Informationsgesellschaft — Quo vaditis?, AJP 2013, 1423 ff., der insbesondere auf die Frage des massgeblichen Beurteilungshorizonts eingeht, dies auch aus rechtsvergleichender Sicht.

Person aufgrund der zur Verfügung stehenden Angaben, so dass es letztlich darauf ankommen dürfte, ob eine Wiederherstellung derjenigen Daten, die die Anonymisierung rückgängig machen können, nur noch mit einem solch hohen Aufwand erfolgen kann, dass nicht anzunehmen ist, dass dieser in Kauf genommen wird.[13] Auch hier stellt sich ggf. das Problem, dass sich der Aufwand für eine Rückgängigmachung der Anonymisierung mit der technischen Entwicklung reduzieren kann, so dass die Frage, ob bestimmte Daten Personendaten sind oder nicht, auch in diesem Zusammenhang nicht zu einem bestimmten Zeitpunkt endgültig beantwortet werden kann, sondern regelmässig neu zu beurteilen ist.

[Rz 13] Bei pseudonymisierten Daten gibt es bereits *per definitionem* noch einen Zuordnungsschlüssel, so dass das Datenschutzrecht immer dann Anwendung findet, wenn der Bearbeiter den Zuordnungsschlüssel kennt oder die Entschlüsselung grundsätzlich möglich ist.[14]

b) In Bezug auf Big Data

[Rz 14] Wendet man die skizzierten Grundsätze auf *Big Data* an, so kann Folgendes festgehalten werden:

- Soweit es um Datenbearbeitungen geht, die sich «direkt» auf personenbezogene Daten beziehen, ohne dass diese in irgendeiner Form anonymisiert oder auch nur pseudonymisiert werden (wie dies z.B. bei der Überwachung von Online-Zahlungsdiensten im Hinblick auf die Betrugsbekämpfung oder bei der Analyse von Kundendaten häufig der Fall sein wird), ist das Vorliegen personenbezogener Daten unproblematisch zu bejahen.
- Soweit sich *Big Data* auf «endgültig» anonymisierte Daten bezieht, ist ein Personenbezug zu verneinen, und das Datenschutzrecht kommt nicht zur Anwendung. Zu beachten ist jedoch, dass diese Fallgestaltung nur dann anzunehmen ist, wenn die Anonymisierung in der Tat irreversibel ist, so dass es auch nicht mehr vorstellbar ist, die Anonymisierung durch den Einsatz weiterer technischer Mittel bzw. im Falle einer Weiterentwicklung derselben rückgängig zu machen. Deutlich wird damit auch, dass diese Voraussetzung im Zusammenhang mit *Big Data* häufig nicht bejaht werden kann, wird es doch in zahlreichen Konstellationen möglich sein, zumindest gewisse Daten durch den Einsatz weiterentwickelter Algorithmen sowie den Einbezug zusätzlicher Angaben dann doch wieder bestimmten Personen zuzuordnen. So ist es etwa in Bezug auf Gesundheitsdaten einer Reihe von Personen, die insofern anonymisiert werden, als die Namen von den Dossiers entfernt werden, denkbar, dass über eine Verknüpfung der verbleibenden Daten (z.B. Alter, Gesundheitszustand, Wohnort u.a.m.) mit anderen Daten zumindest gewisse dieser Daten wieder auf bestimmte Personen bezogen werden (können).
- Vor diesem Hintergrund wird es bei *Big Data* in der Regel denkbar sein, dass zunächst anonyme oder anonymisierte Daten gerade durch den Einsatz von *Big Data* re-individualisiert werden (können).[15] Deutlich wird damit, dass die Anwendbarkeit des Datenschutzrechts

[13] Ähnlich wohl auch Probst, in: Datenverknüpfung (Fn. 9), 1 (13 ff.). Vgl. im Zusammenhang mit *Big Data* auch noch unten III.1.b).

[14] Vgl. Stefan Gerschwiler, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in: Nicolas Passadelis/David Rosenthal/Hanspeter Thür (Hrsg.), Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, §3, Rz. 3.31 f.; Probst, in: Datenverknüpfung (Fn. 9), 1 (17 f.).

[15] Vgl. insoweit Baeriswyl, in: Big Data und Datenschutz (Fn. 3), 45 (51 f.), mit einigen Beispielen.

von der oben[16] bereits erörterten Frage abhängt, ob angesichts der zur Verfügung stehenden Mittel und der involvierten Interessen davon auszugehen ist, dass eine derartige Re-Individualisierung erfolgt oder doch zumindest mit einer solchen Re-Individualisierung zu rechnen ist. Ist diese Frage zu bejahen, ist nach der hier vertretenen Ansicht davon auszugehen, dass es sich um Daten handelt, die sich auf bestimmbare Personen beziehen. Denn ob die Bestimmbarkeit «einfach» gegeben ist, also die Person aufgrund des Datums oder der Daten auch ohne den Rückgriff auf technische Mittel oder unter Verwendung «einfacher» technischer Mittel bestimmbar ist, oder ob dies erst unter Einsatz komplexerer Vorgänge — eben *Big Data* — möglich ist, ist *per se* aus rechtlicher Sicht nicht grundsätzlich relevant. Die Notwendigkeit des Einsatzes komplexer Informationstechnologie kann jedoch bei der Frage von Bedeutung sein, ob damit gerechnet werden kann, dass eine derartige Re-Individualisierung erfolgt. Dies wird umso eher der Fall sein, wenn die Datenbearbeitung gerade darauf ausgerichtet ist, die Re-Individualisierung zu erreichen, dürfte diese doch oftmals einen wichtigen Zweck von *Big Data* darstellen. Mit der Ausbreitung der Anwendung von *Big Data* und der Weiterentwicklung der technischen Möglichkeiten erhöht sich die Wahrscheinlichkeit der Bestimmbarkeit von Personen aufgrund zunächst anonym erscheinender Daten jedoch auch generell. Daher erscheint es zumindest im Zusammenhang mit *Big Data* nicht (mehr) zutreffend, allgemein zu formulieren, das Datenschutzgesetz sei auf die Bearbeitung anonymer Daten nicht anwendbar. Vielmehr ist positiv zu formulieren, dass eine Bearbeitung personenbezogener Daten von vornherein auch dann vorliegt, wenn *a priori* anonyme bzw. anonymisierte Daten bearbeitet werden und damit zu rechnen ist, dass diese Bearbeitung zu einer Re-Individualisierung führt; bei Vorliegen dieser Voraussetzungen handelt es sich dann eben nicht mehr um anonyme Daten in dem Sinn, dass eine Bestimmbarkeit der betroffenen Personen nicht gegeben wäre. Die Möglichkeit oder gar Wahrscheinlichkeit einer solchen Re-Individualisierung steigt mit den herangezogenen Datenmengen sowie der Verfeinerung der Algorithmen tendenziell immer mehr an.

[Rz 15] Aber auch diese Präzisierungen ändern letztlich nichts daran, dass es häufig unklar sein wird, ob das Datenschutzrecht auf *Big Data* zum Zeitpunkt seines Ersteinsatzes Anwendung findet, da die Vorhersehbarkeit einer derartigen Re-Individualisierung in aller Regel mit gewissen Unsicherheiten behaftet ist, ganz abgesehen davon, dass es auch «unbeabsichtigt» im Zuge der Analyse zu solchen Re-Individualisierungen kommen kann (sind doch die Ergebnisse von *Big Data*-Analysen mitunter nicht oder nur schwer vorhersehbar).

[Rz 16] Gesichert ist jedoch, dass das Datenschutzrecht jedenfalls ab dem Zeitpunkt, da die Re-Individualisierung erfolgt ist, also sich das Datum auf eine bestimmbare Person bezieht, Anwendung findet.

[Rz 17] Die vorstehenden Erwägungen implizieren somit, dass es denkbar ist, dass das Datenschutzrecht zum Zeitpunkt des Beginns einer *Big Data*-Analyse nicht anwendbar ist, sich dies jedoch im Laufe der Zeit ändert, etwa wenn gewisse Daten im Laufe der Analyse bestimmbaren Personen zugeordnet werden können oder sich die technischen Möglichkeiten so weiterentwickeln, dass die Bestimmbarkeit — im Gegensatz zu einem früheren Zeitpunkt — mittlerweile bejaht werden kann. In der Konsequenz bedeutet dies, dass bei der Bearbeitung von Daten im Rahmen von *Big Data* das Datenschutzgesetz (und damit die datenschutzrechtlichen Grundsätze

16 III.1.a).

in Art. 4 DSG) wegen des fehlenden Personenbezugs zunächst keine Anwendung finden kann, dies obwohl gerade die Bearbeitung möglicherweise in einer De-Anonymisierung resultiert, diese aber nicht vorhersehbar war oder mit dieser nicht gerechnet werden musste. Damit ist es aufgrund der geltenden Rechtslage *a priori* denkbar, dass in dem Zeitraum zwischen dem Abschluss der Anonymisierung und der Herstellung des Personenbezugs das Datenschutzrecht gerade keine Anwendung findet.

2. Zur Tragweite ausgewählter datenschutzrechtlicher Grundsätze im Zusammenhang mit Big Data

[Rz 18] Die vorstehenden Ausführungen vermochten zu illustrieren, dass das Datenschutzgesetz auch im Zusammenhang mit *Big Data* zum Zuge kommen kann, dies soweit — unter Heranziehung der ausgeführten Grundsätze[17] — die Bearbeitung personenbezogener Daten zur Debatte steht. Diesfalls sind somit die Vorgaben des Datenschutzgesetzes, insbesondere die allgemeinen Grundsätze des Art. 4 DSG sowie die spezifischen Voraussetzungen der Rechtmässigkeit der Datenbearbeitung, die jeweils in Bezug auf Private (Art. 12 ff. DSG) sowie öffentliche Organe (Art. 16 ff. DSG) zum Zuge kommen, zu beachten. Spezifische Fragen werden in diesem Zusammenhang dann aufgeworfen, wenn es sich um die oben skizzierte Konstellation handelt, in der sich *Big Data* auf zunächst anonyme oder anonymisierte Daten bezieht, eine Re-Identifikation jedoch nicht ausgeschlossen erscheint. Vor diesem Hintergrund geht es im Folgenden darum, die Relevanz ausgewählter datenschutzrechtlicher Grundsätze (im Vordergrund stehen hierbei die Grundsätze der Rechtmässigkeit, der Transparenz und der Zweckbindung) in diesem Zusammenhang aufzuzeigen, wobei zwischen ihrer Heranziehung bereits zu Beginn der Datenbearbeitung einerseits (a) sowie nach einer effektiv erfolgten Re-Individualisierung andererseits (b) zu unterscheiden ist.

a) Tragweite ausgewählter datenschutzrechtlicher Grundsätze «ab initio»

[Rz 19] Nach dem Gesagten[18] fällt eine Datenbearbeitung im Rahmen von *Big Data* auch dann in den Anwendungsbereich des Datenschutzgesetzes, wenn an sich zunächst anonyme bzw. anonymisierte Daten bearbeitet werden, jedoch damit zu rechnen ist, dass diese Bearbeitung zu einer Re-Individualisierung führt. Dieser Ansatz impliziert, dass die datenschutzrechtlichen Grundsätze bereits vor einer eigentlichen Re-Individualisierung zum Zuge kommen und zu beachten sind, was in der konkreten Rechtsanwendung durchaus Probleme aufwerfen kann. Die Tragweite der datenschutzrechtlichen Grundsätze muss denn auch notwendigerweise unter Berücksichtigung dieser spezifischen Konstellation präzisiert werden, was im Folgenden für die Grundsätze der Rechtmässigkeit (aa), der Transparenz (bb) und der Zweckbindung (cc) skizziert werden soll.

[17] III.1.

[18] Oben III.1.

aa) Grundsatz der Rechtmässigkeit

[Rz 20] Nach Art. 4 Abs. 1 DSG dürfen Personendaten nur rechtmässig bearbeitet werden, so dass die Bearbeitung nicht gegen eine in der Schweiz geltende Rechtsnorm verstossen darf.[19] Dieser Grundsatz wird für Private in Art. 12 ff., für Bundesorgane in Art. 16 ff. DSG spezifiziert:

[Rz 21] Bei Privaten muss im Falle der Bearbeitung von Personendaten grundsätzlich ein Rechtfertigungsgrund vorliegen. Dieser kann in Bezug auf *Big Data* insbesondere einerseits in einem überwiegenden privaten Interesse liegen, andererseits auf einer Einwilligung der Betroffenen beruhen.

- Die Frage nach dem Vorliegen eines überwiegenden privaten Interesses ist dabei in Bezug auf die konkret vorgenommene Bearbeitung im Rahmen von *Big Data* zu beantworten, wobei einerseits das Interesse an der Bearbeitung, andererseits die Schwere des Eingriffs in die Persönlichkeitsrechte der Betroffenen zu berücksichtigen sind.
- Eine gültige Einwilligung kann nur unter den Voraussetzungen des Art. 4 Abs. 5 DSG vorliegen, so dass sie insbesondere nach angemessener Information und freiwillig erfolgen muss. Im Rahmen von *Big Data* wird eine Einwilligung jedoch häufig an der hinreichenden Informiertheit scheitern: Diese setzt nämlich voraus, dass die Betroffenen nicht nur über die Datenbearbeitung an sich, sondern auch über die Prozesse, den Umfang und die Zwecke in hinreichend transparenter Weise informiert sein müssen,[20] was bei *Big Data* wohl nur ausnahmsweise gegeben sein wird, dies nicht nur, soweit es um (zunächst) anonyme oder anonymisierte Daten geht, sondern auch soweit im Rahmen von *Big Data* direkt personenbezogene Daten bearbeitet werden.[21] Bei zunächst anonymen oder anonymisierten Daten dürfte eine Einwilligung von vornherein grundsätzlich nicht in Betracht kommen, da ja nicht ersichtlich ist, wer einzuwilligen hat; Ausnahmen mögen für Einwilligungen im Vorfeld der Anonymisierung denkbar sein (etwa im Zusammenhang mit Gesundheitsdaten), wobei auch hier dann die hinreichende Information problematisch sein kann.[22]

[Rz 22] Soweit öffentliche Organe betroffen sind, wird der Grundsatz der Rechtmässigkeit in Art. 17 DSG insoweit präzisiert, dass diese Personendaten grundsätzlich nur bearbeiten dürfen, wenn hierfür eine gesetzliche Grundlage besteht.[23] Somit dürfen öffentliche Organe nur dann

---

19 Vgl. allgemein zu diesem Grundsatz Astrid Epiney, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011, §9, Rn. 11 ff., m.w.N.

20 Vgl. nur, m.w.N., Epiney, in: Datenschutzrecht (Fn. 19), §9, Rn. 17.

21 S. in diesem Zusammenhang aus rechtsvergleichender Sicht etwa ein Urteil des LG Berlin, in dem es um die Rechtmässigkeit einer Einwilligung in Bezug auf eine Datenbearbeitung ging, die in sehr allgemeiner Form umschrieben worden war; so war in der Datenschutzerklärung das Recht eingeräumt worden, «Daten auch mit anderen Informationen (zu) verbinden, um unsere Produkte, Dienstleistungen, Inhalte und Werbung anzubieten oder zu verbessern» sowie «Daten auch für interne Zwecke zu nutzen, wie zur Datenanalyse und Forschung, um Produkte, Dienste und Kommunikation mit Kunden zu verbessern». Es handle sich hier um eine Art globale Einwilligung in Datenbearbeitungsprozesse, die in ihrem Umfang den Betroffenen nicht hinreichend bekannt sein könnten, ganz abgesehen davon, dass die Zwecke nicht ausreichend erläutert worden seien, vgl. LG Berlin, NJW 2013, 2605. Zu diesem Urteil z.B. Jan-Peter Ohrtmann/Sebastian Schwiering, Big Data und Datenschutz — Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, 2984 (2988 f.).

22 Ein hier nicht näher zu behandelndes Sonderproblem ist dasjenige, ob der Umstand, dass jemand seine Personendaten selbst (insbesondere auf dem Internet) allgemein zugänglich gemacht hat, eine gültige Einwilligung auch in ihre Nutzung im Rahmen von *Big Data* impliziert. Zweifel sind hier angebracht, und auch Art. 12 Abs. 3 DSG sieht immerhin vor, dass eine Persönlichkeitsverletzung im Falle der durch die Person selbst vorgenommenen Veröffentlichungen nur «in der Regel» zu verneinen ist. Dies impliziert, dass auch im Falle der Bearbeitung öffentlich zugänglicher Daten jeweils eine Interessenabwägung vorzunehmen ist. Ähnlich etwa Thilo Weichert, Big Data und Datenschutz, ZD 2013, 251 (257).

23 Ausführlich hierzu Bernhard Waldmann, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann, Datenschutz-

auf *Big Data* zurückgreifen (immer unter der Voraussetzung, dass die Anwendbarkeit des Datenschutzgesetzes zu bejahen ist), wenn eine entsprechende gesetzliche Grundlage — die ihrerseits hinreichend präzise sein muss — besteht. Die Voraussetzungen für die Surrogate einer gesetzlichen Grundlage (Art. 17 Abs. 2 DSG)[24] dürften im Falle von *Big Data* — wenn überhaupt — nur ausnahmsweise zu bejahen sein.

[Rz 23] Verpflichtet ist jedenfalls der Datenbearbeiter, also derjenige, der *Big Data* einsetzt. Daneben sind aber auch diejenigen verpflichtet, die anonymisierte Daten veröffentlichen (die Bekanntgabe von Daten ist eine Form der Datenbearbeitung, vgl. die Legaldefinition in Art. 3 lit. e DSG), jedoch damit zu rechnen ist, dass Dritte durch die Verwendung von *Big Data* eine Re-Individualisierung vornehmen (können). Diesfalls handelt es sich eben nicht mehr um anonyme Daten, sondern um Daten über bestimmbare Personen.[25] Wenn also z.B. unter dem Stichwort «*Open Government Data*» gewisse Daten in an sich anonymisierter Form (im Internet) veröffentlicht werden, sich die publizierten Daten aber unter Heranziehung weiterer Daten mit einem überschaubaren Aufwand bestimmten Personen zuordnen lassen, sind die Betroffenen bestimmbar, so dass es diesfalls eben doch um Personendaten geht, dies mit der Folge, dass das Datenschutzgesetz anwendbar ist und — da es sich hier um die Bekanntgabe durch öffentliche Organe handelt — für die Veröffentlichung eine gesetzliche Grundlage erforderlich ist.

bb) Grundsatz der Transparenz

[Rz 24] Gemäss Art. 4 Abs. 4 DSG muss die Beschaffung von Personendaten, insbesondere der Zweck ihrer Bearbeitung, für die betroffene Person erkennbar sein. Art. 14 und 18a DSG präzisieren diesen Grundsatz für öffentliche Organe und Private. Bei *Big Data* bringt die effektive Beachtung dieses Grundsatzes gewisse Herausforderungen mit sich: Eine eigentliche Erkennbarkeit der Datenbearbeitung dürfte — von Ausnahmefällen abgesehen — angesichts der Komplexität der Datenbearbeitung im Rahmen von *Big Data* in aller Regel zu verneinen sein. Daher kann dem Grundsatz der Transparenz letztlich nur über eine hinreichende Information Rechnung getragen werden, die ihrerseits genügend präzise zu sein hat, wobei hier ähnliche Herausforderungen bestehen wie sie im Zusammenhang mit der Einwilligung skizziert wurden.[26] Hinzu kommt eine Schwierigkeit bei der Bearbeitung zunächst anonymer bzw. anonymisierter Daten: Da der für die Datenbearbeitung Verantwortliche hier zu Beginn der Datenbearbeitung noch nicht weiss, wessen Daten er bearbeitet, kann er die Betroffenen auch nicht informieren. Fraglich ist daher in diesem Zusammenhang, ob dieser Umstand *per se* zu einer Unzulässigkeit der Datenbearbeitung führt. Die besseren Gründe dürften für eine Verneinung dieser Frage sprechen: Denn dem Datenbearbeiter im Rahmen von *Big Data* ist es aufgrund der noch bestehenden Anonymisierung der Daten nicht möglich, eine solche Information vorzunehmen, und gesetzliche Pflichten dürfen nicht so ausgelegt werden, dass ihre Erfüllung unmöglich ist *(ad impossibilia nemo tenetur)*, was aber die Konsequenz der Bejahung der aufgeworfenen Frage wäre. Dies ändert freilich nichts daran, dass der Grundsatz von Treu und Glauben, ggf. i.V.m. Art. 4 Abs. 4 DSG, wohl impliziert, dass

---

recht. Grundlagen und öffentliches Recht, Bern 2011, §12, Rn. 41 ff.

24 Vgl. hierzu, m.w.N., Astrid Epiney, Besonders schützenswerte Personendaten — Zu den Anforderungen an die Rechtmässigkeit der Bearbeitung durch öffentliche Organe im Falle des Fehlens einer gesetzlichen Grundlage, FS Paul-Henri Steinauer, 2014, 97 ff.

25 S.o. III.1.

26 S.o. III.2.a)aa).

die Datenbearbeiter die Betroffenen zu informieren haben, sobald eine Re-Identifikation erfolgt ist.[27]

cc) Grundsatz der Zweckbindung

[Rz 25] Nach dem in Art. 4 Abs. 3 DSG verankerten Grundsatz der Zweckbindung dürfen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.[28] Mit der Zweckbindung soll einerseits erreicht werden, dass der Zweck für die betroffene Person bereits bei der Beschaffung der Daten ersichtlich ist. Andererseits soll verhindert werden, dass die Daten für andere Zwecke verwendet werden, als bei der Beschaffung absehbar war (keine «Zweckentfremdung»[29]).[30] Diese «enge Zweckbindung»[31] wird insofern relativiert, als der Zweck inhaltlich weit gefasst werden kann.[32] Der Zweckbindungsgrundsatz impliziert u.a., dass der Zweck der Datenbearbeitung im Vorfeld bekannt sein muss. Auch verstösst grundsätzlich eine Datenbeschaffung ohne Zweckhintergrund gegen dieses Prinzip, so dass die Beschaffung von Personendaten «auf Vorrat», in der Annahme, irgendwann könne man sie schon für irgendetwas gebrauchen, unzulässig ist.[33]

[Rz 26] Da es bei *Big Data* schon definitionsgemäss um die Verknüpfung einer Vielzahl von Daten geht, um neue Informationen zu generieren, wobei der Zweck mitunter im Voraus bekannt ist, mitunter der zukünftige Bearbeitungszweck aber auch davon abhängt, welche Daten überhaupt neu ermittelt werden können, steht *Big Data* in einem unübersehbaren Spannungsverhältnis zum Zweckbindungsgrundsatz, dies auch und gerade soweit es um die Bearbeitung zunächst anonymisiert erscheinender Daten geht.[34] Gleichwohl erscheint es wenig plausibel, bereits auf dieser Grundlage eine grundsätzliche Unzulässigkeit von *Big Data* anzunehmen (wobei auch hier zunächst nur die Situation der Bearbeitung zunächst anonymisiert erscheinender Daten berücksichtigt wird):

- Soweit es um das dem Zweckbindungsgrundsatz an sich inhärente Erfordernis geht, dass der Zweck der Datenbearbeitung bei der Datenbeschaffung erkennbar sein muss, kann auf die oben im Zusammenhang mit dem Transparenzgrundsatz angestellten Überlegungen[35] verwiesen werden: In der Regel wird die Datenbearbeitung für die Betroffenen in ihrem vollen Umfang nicht erkennbar sein, und eine hinreichend vollständige Information erscheint angesichts des Umstands, dass die Daten zunächst anonym bzw. anonymisiert waren, von vornherein ausgeschlossen. Allerdings kann hieraus wegen des Grundsatzes *ad impossibilia nemo tenetur* kein Verstoss gegen datenschutzrechtliche Vorgaben resultieren.
- Im Übrigen erscheint es auch bei *Big Data* durchaus möglich, Zwecke der Datenbearbeitung

[27] S. insoweit auch noch unten III.2.b).

[28] S. im Einzelnen zu diesem Grundsatz, m.w.N., Epiney, in: Datenschutzrecht (Fn. 19), §9, Rn. 29 ff.

[29] Astrid Epiney/Daniela Nüesch, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in: Nicolas Passadelis/David Rosenthal/Hanspeter Thür (Hrsg.), Datenschutzrecht, Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, §3, Rz. 3.82.

[30] Thouvenin, in: Big Data und Datenschutz (Fn. 3), 62 (75).

[31] Thouvenin, in: Big Data und Datenschutz (Fn. 3), 62 (67).

[32] Aus der Rechtsprechung etwa Urteil des Bundesgerichts 2A.692/2006 vom 1. Februar 2007.

[33] S. nur, m.w.N. aus Literatur und Rechtsprechung, Epiney, in: Datenschutzrecht (Fn. 19), §9, Rn. 33.

[34] Zum Problemkreis ausführlich etwa Thouvenin, in: Big Data und Datenschutz (Fn. 3), 62 (67 ff.).

[35] III.2.a)bb).

im Vorfeld zu definieren und die Datenbearbeitung und damit auch die verwendeten Algorithmen an diesen auszurichten.

[Rz 27] Damit kann der Zweckbindungsgrundsatz in unserem Zusammenhang dahingehend konkretisiert werden, dass sicherzustellen ist, dass der Zweck des Rückgriffs auf *Big Data* (z.B. Verhinderung von Terroranschlägen, Bekämpfung der Manipulation im Börsenhandel oder neue wissenschaftliche Erkenntnisse in Bezug auf bestimmte Fragen) im Vorfeld hinreichend bestimmt definiert wird und der konkrete Einsatz von *Big Data* und damit auch die Algorithmen in Abhängigkeit von gerade diesem Zweck definiert werden. Gleichzeitig ist damit auch gesagt, dass *Big Data* dann nicht mit dem Zweckbindungsgrundsatz in Einklang steht, wenn der Einsatz «blind» und damit ohne eine hinreichend präzise Zielsetzung erfolgt. Die Realität des Rückgriffs auf *Big Data* dürfte diesem Umstand wohl nicht Rechnung tragen.

b) Tragweite ausgewählter datenschutzrechtlicher Grundsätze «ex post»

[Rz 28] Wie bereits erwähnt,[36] ist das Datenschutzgesetz zweifellos umfassend auf alle Daten anwendbar, die im Zuge von *Big Data* als Personendaten im Sinne des Datenschutzgesetzes anzusehen sind. Dies gilt — unabhängig davon, ob das Datenschutzgesetz bereits von vornherein aufgrund der vorhersehbaren oder möglichen Re-Identifizierung scheinbar anonymer Daten auf *Big Data* anwendbar war oder nicht — in jedem Fall für eine im Gefolge von *Big Data* erfolgte Re-Identifizierung zunächst anonymer oder anonym erscheinender Daten. Die datenschutzrechtlichen Grundsätze sind somit in dieser Konstellation vollumfänglich massgeblich. Ihre Relevanz in diesem Stadium dürfte kaum zu überschätzen sein, und ihr kann vorliegend nicht im Einzelnen nachgegangen werden, zumal in diesem Zusammenhang selbstredend auch die Umstände des Einzelfalls relevant sind, was auch und gerade angesichts der Vielfalt der Datenbearbeitungen im Zuge von *Big Data* von grosser Bedeutung ist. Hingewiesen sei aber zur Illustration auf folgende Aspekte:

- Jede weitere Bearbeitung der Daten hat den Grundsätzen der Rechtmässigkeit zu genügen, so dass für Private ein Rechtfertigungsgrund und für öffentliche Organe eine gesetzliche Grundlage notwendig ist.
- Der Grundsatz von Treu und Glauben dürfte implizieren, dass die Betroffenen im Falle einer Re-Individualisierung zu informieren sind.
- Jede weitere Datenbearbeitung (worunter auch die Aufbewahrung fällt, vgl. Art. 3 lit. e DSG) muss den Anforderungen der Transparenz genügen.

[Rz 29] Klarzustellen ist gleichzeitig auch, dass in der Konstellation, in der es sich zu Beginn der Datenbearbeitung um anonyme bzw. anonymisierte Daten handelt und eine Re-Identifizierung weder vorhersehbar noch möglich erscheint, das Datenschutzgesetz zunächst nicht anwendbar ist, so dass seine Vorgaben zu diesem Zeitpunkt nicht verletzt werden können. An dieser Beurteilung ändert sich auch dann nichts, wenn eine Re-Identifizierung später wider Erwarten erfolgt; m.a.W. wird durch diese spätere Re-Individualisierung eine zunächst rechtmässige Datenbearbeitung, die wegen fehlendem Personenbezug nicht unter das Datenschutzgesetz fällt, nicht *ex post* rechtswidrig.

[36] III.1.b).

IV. Schluss

[Rz 30] Die Ausführungen lassen zweierlei erkennen:

- Erstens sind dem geltenden Datenschutzgesetz durchaus Anforderungen zu entnehmen, die im Zusammenhang mit *Big Data* relevant sind. Dies hängt u.a. damit zusammen, dass der Anwendungsbereich des Datenschutzgesetzes im Zusammenhang mit *Big Data* weiter gezogen ist, als man auf den ersten Blick annehmen könnte. Zwar stösst die Anwendung der datenschutzrechtlichen Grundsätze auf *Big Data* durchaus auf gewisse Schwierigkeiten, ist doch das Gesetz nicht auf diesen Anwendungsfall hin konzipiert. Nichtsdestotrotz dürfte es durchaus ein «griffiges Raster»[37] zur Verfügung stellen, mit dem sich eine Reihe von Herausforderungen, die mit *Big Data* einhergehen, bewältigen lassen. Insofern setzt das geltende Datenschutzrecht der Datenbearbeitung im Rahmen von *Big Data* beachtliche Grenzen, die insbesondere vorstehend nicht weiter vertieften Konstellationen, in denen sich *Big Data* von vornherein und zweifelsfrei auf Personendaten bezieht, von Bedeutung sein dürften. Dass die gelebte Wirklichkeit den rechtlichen Anforderungen in zahlreichen Konstellationen nicht Rechnung tragen dürfte, ändert hieran nichts. Zwar mögen die datenschutzrechtlichen Grundsätze angesichts u.a. von *Big Data* als ein Relikt aus vergangenen Zeiten erscheinen, die der modernen Informationstechnologie nicht ausreichend Rechnung tragen. Nach der hier vertretenen Ansicht sind sie aber Ausdruck grundlegender Anforderungen, die sich aus den Persönlichkeitsrechten ableiten lassen, deren Beachtung gerade angesichts des mit *Big Data* einhergehenden Gefährdungspotentials für die Persönlichkeitsrechte nicht nur nach wie vor aktuell, sondern auch unentbehrlich erscheint.
- Zweitens ist jedoch nicht zu verkennen, dass die genaue Tragweite des Datenschutzgesetzes in diesem Zusammenhang gewissen Unsicherheiten unterworfen ist. Diese sind zunächst darin begründet, dass die allgemeinen datenschutzrechtlichen Grundsätze auf die besondere Konstellation der Verwendung von *Big Data* angewandt werden müssen, so dass deren Tragweite letztlich insofern präzisiert werden muss. Eine solche Anwendung allgemeiner Grundsätze auf eine besondere Fallgestaltung kann aber — und die vorangegangenen Ausführungen konnten dies wohl auch etwas illustrieren — durchaus mit den üblichen juristischen Methoden bewerkstelligt werden. Von grösserer Bedeutung erscheint daher der zweite Hauptunsicherheitsfaktor in diesem Zusammenhang: Die Frage, ob das Datenschutzgesetz anwendbar ist oder nicht, ist aufgrund der Eigenart von *Big Data* mit ausgesprochen grossen Unsicherheiten behaftet, die noch zu denjenigen hinzukommen, die dem Begriff der «bestimmbaren» Person sowieso schon inhärent sind.[38] Denn die Frage, ob ein Datum ein Personendatum ist, hängt von der Bestimmbarkeit ab, die im Falle zunächst anonym erscheinender Daten nach dem Gesagten[39] auch dann gegeben sein kann, wenn damit zu rechnen ist, dass durch *Big Data* eine Re-Individualisierung erfolgen kann. Ob diese Voraussetzung jedoch vorliegt, ist sehr grossen Unsicherheiten unterworfen. Nicht mit dem geltenden Recht in Einklang stehend dürfte es aber jedenfalls sein, den Begriff der Personendaten so auszulegen, dass potentiell alle Daten persönlich bestimmbar sind, so dass es keine anonymisierten Daten bzw. im

[37] Vgl. diesen Ausdruck bei Herbert Burkert, Aktuelle Herausforderungen des Datenschutzrechts, in: Astrid Epiney/Tobias Fasnacht/Gaëtan Blaser (Hrsg), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich 2013, 1 (17).

[38] Zu letzteren instruktiv Probst, AJP 2013 (Fn. 12), 1423 ff.

[39] Oben III.1.

Grunde allgemein keine Sachdaten mehr geben könnte,[40] so dass die Abgrenzungsfrage — die ganz entscheidend ist, hängt die Anwendbarkeit des Datenschutzgesetzes doch von ihrer Beantwortung ab — bleibt. Hinzu kommt, dass im Falle der Verneinung der Anwendbarkeit der Datenschutzgesetzgebung auf gewisse Operationen im Bereich von *Big Data* und einer anschliessenden Re-Individualisierung und somit einer erneuten Anwendbarkeit der datenschutzrechtlichen Grundsätze aufgrund der vorübergehenden «Anwendungslücke» Inkonsistenzen auftreten könnten, die im Wesentlichen in den damit einhergehenden Unterschieden der in den verschiedenen Stadien der Datenbearbeitung massgeblichen rechtlichen Vorgaben bestehen. Schliesslich erscheint es auch nicht gänzlich ausgeschlossen, dass solche «Anwendungslücken» dazu genützt würden, um zum entsprechenden Zeitpunkt datenschutzrechtlich problematische Bearbeitungen vorzunehmen und somit die entsprechenden Standards des Datenschutzrechts zu umgehen.

[Rz 31] Will man den personenbezogenen Ansatz des Datenschutzrechts nicht aufgeben (wofür übrigens schon deshalb wenig spricht, weil dieser ein Ausfluss des Grundrechts auf Schutz der Persönlichkeit ist, das einen ganz anderen Stellenwert hat als das möglicherweise gegebene öffentliche Anliegen, allgemein den Umgang mit Daten zu regeln), so drängt sich vor diesem Hintergrund die Frage auf, ob das Datenschutzrecht nicht durch ein (schlankes) «Datenrecht» ergänzt werden sollte; hingegen erscheint es wegen des erwähnten Grundrechtsbezugs wenig zielführend, das Datenschutzrecht durch ein solches «Datenrecht» zu ersetzen. Ein Datenrecht käme als Mindeststandard für jegliche Formen der Datenbearbeitung zur Anwendung, während das Datenschutzrecht besondere, wegen der (grösseren) Grundrechtsrelevanz auch weitergehende Anforderungen stellte. Der Regelungsinhalt könnte sich durchaus an den datenschutzrechtlichen Grundsätzen orientieren, müsste diese jedoch in geeigneter Weise anpassen und ergänzen. Zu denken wäre dabei insbesondere an spezifische Regelungen der Vorabkontrolle, abgestuft nach dem Gefährdungspotential, die Spezifizierung von Informationspflichten sowie die Präzisierung des Zweckbindungsgrundsatzes. Ein solches Datenrecht könnte zwar die skizzierten Schwierigkeiten bei der Bestimmung des Anwendungsbereichs des Datenschutzrechts nicht gänzlich vermeiden; jedoch implizierte es die Geltung gewisser Grundregeln auch für den Fall der Verneinung der Anwendbarkeit des Datenschutzrechts, womit zumindest die Auswirkungen einer solchen Verneinung reduziert würden.

[Rz 32] Darüber hinaus gilt es, die bestehenden rechtlichen Grundsätze konsequent anzuwenden und insbesondere auch technische und organisatorische Lösungen zu entwickeln, welche die effektive Beachtung der einschlägigen datenschutzrechtlichen Grundsätze auch im Rahmen von *Big Data* zu gewährleisten vermögen. Diese erscheinen nicht nur für die in diesem Beitrag besonders im Vordergrund stehende Bearbeitung *a priori* anonymer Daten, sondern auch und gerade für die Bearbeitung von Daten, bei denen der Anwendungsbereich des Datenschutzgesetzes zweifellos eröffnet ist, von grosser Bedeutung.

Astrid Epiney, Professorin für Europarecht, Völkerrecht und öffentliches Recht an der Universität Freiburg i.Ü. und Rektorin der Universität.

[40] S. insoweit auch Baeriswyl, in: Big Data und Datenschutz (Fn. 3), 45 (55); Baeriswyl, digma 1/2013 (Fn. 11), 14 (15 f.).

Die Verfasserin dankt Herrn *Marcel Stucky* für die Unterstützung bei der Erstellung dieses Beitrags. Dr. *Markus Kern* sei für die kritische Durchsicht des Manuskripts sowie die Anregungen herzlich gedankt.