A. Big Data und die Forderung nach Datenqualität (Thomas Hoeren)

Auf einen Blick: Big Data und Datenqualität

Big Data ist eng mit der neuen, alten Frage der Datenqualität verknüpft. Wenn eine neue Forschungsperspektive wie Big Data gerade darauf aufsetzt, irrelevante Daten ungefiltert auszuwerten, muss sich auch die Frage nach der Datenqualität stellen. Dafür spricht auch, dass die EU-DSGVO die Einhaltung von Datenqualitätsstandards zu einer bußgeldsanktionierten Forderung an Datenverarbeiter erhebt. Doch was bedeutet Datenqualität? Wie passt diese Forderung ins System des allgemeinen Zivilrechts und in die Struktur des Datenschutzrechts?

I. Einführung

Die Forderung nach Datenqualität ist alt.[1] Schon die EU-Datenschutzrichtlinie enthielt in Art. 6 unter der Rubrik „Datenschutzgrundsätze" ein Prinzip, wonach personenbezogene Daten „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein" müssten. Allerdings fehlte bei dieser Forderung jedwede Sanktion. Es kann daher nicht verwundern, dass der deutsche Gesetzgeber im BDSG die Grundsätze gar nicht umsetzt[2] (anders als Österreich[3] oder die Schweiz[4]). Umso bedeutungsloser dürfte die Forderung in der datenverarbeitenden Wirtschaft zumindest in Deutschland aufgenommen worden sein.

Das Schweigen des deutschen Rechts verblüfft allerdings, wenn man sich die aktuelle Bedeutung von Art. 6 EU-Datenschutzrichtlinie in der rechtspolitischen Diskussion ansieht. Nicht ohne Grund betont der EuGH

---

[1] Fußnoten beziehen sich im Weiteren nur auf die zum Verständnis des Textes notwendigen Belege.

[2] Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 22. Mai 2001 (BGBl. I S. 904).

[3] § 6 des Bundesgesetzes über den Schutz personenbezogener Daten, (BGBl. I Nr. 165/1999.

[4] Art. 5 des Schweizerischen DSG vom 19. Juni 1992, AS 1993, 1945.

im Google-Urteil die Grundsätze der Datenqualität. Jede Verarbeitung personenbezogener Daten müsse den in Art. 6 der Richtlinie aufgestellten Grundsätzen in Bezug auf die Qualität der Daten genügen (Rdnr. 73).[5] Aus dem Grundsatz der Datenrichtigkeit ergebe sich auch, „dass auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten im Laufe der Zeit nicht mehr den Bestimmungen der Richtlinie entsprechen kann, wenn die Daten für die Zwecke, für die sie erhoben oder verarbeitet worden sind, nicht mehr erforderlich sind" (Rdnr. 93).

Die Verankerung dieses Prinzips im Datenschutzrecht war allerdings eher unglücklich und wenig durchdacht. Mit Datenschutz hat die Frage der Datenqualität wenig zu tun. Wer (wie der Verfasser) aufgrund überalterter Daten ein äußerst positives, aber leider mit Daten des reichen Onkels vermengtes Scorebild bei der Schufa bekommt, fühlt sich nicht betroffen. Umgekehrt ist nicht einzusehen, warum von der Frage der Datenrichtigkeit nur natürliche Personen betroffen sein sollen. Man denke nur an den Fall Kirchgruppe versus Deutsche Bank und die fatalen Folgen nicht korrekter Hinweise auf die Zahlungsfähigkeit einer Unternehmensgruppe.[6] Insofern ist die Forderung der Datenqualität primär eine Frage des allgemeinen Zivilrechts und nicht des Datenschutzrechts.

Datenqualität ist zunächst einmal etwas, was im Interesse der verarbeitenden Industrie liegt. Das Ziel jeden Datenverarbeiters liegt darin, im eigenen Interesse möglichst viele valide, aktuelle und korrekte Daten zu verarbeiten. In besonders sicherheitsrelevanten Bereichen finden sich daher schon normative Fragmente einer Pflicht zur Gewährleistung der Datenqualität. So gilt für Flugorganisationen europaweit ein entsprechendes Gebot[7]; ähnliches gilt für Statistikbehörden[8] oder Finanzdienstleiter[9].

Das Gebot stellt sich zivilrechtlich vor allem im Hinblick auf die allgemeinen Sanktionen bei der Verwendung falscher Daten. Negative Folgen

---

[5] Vgl. Urteile Österreichischer Rundfunk u. a., EU:C:2003:294, Rdnr. 65; ASNEF und FECEMD, C-468/10 und C-469/10, EU:C:2011:777, Rdnr. 26 und Worten, C-342/12, EU:C:2013:355, Rdnr. 33).

[6] Dazu u.a. BGH, NJW 2006, 830 und *Derleder*, NJW 2013, 1786 ff.; *Höpfner/Seibl*, BB 2006, 673 ff.

[7] Art. 6 der Luftfahrtdaten-Qualitätsanforderungen-Verordnung.

[8] Art. 12 der Verordnung (EG) Nr. 223/2009 vom 11. März 2009, ABl. 2009, Nr. L 87/169.

[9] § 17 Solvabilitätsverordnung vom 14.12.2009, BGBl. I 2926 und § 4 der Versicherungsmeldeverordnung.vom 18.4.2016, BGBl. I S. 793.

für den Betroffenen wurden und werden häufig über Schadensersatzsanktionen aus dem allgemeinen Zivilrecht kompensiert, etwa über § 824 BGB oder die Verletzung vorvertraglicher Sorgfaltspflichten aus § 280 BGB. Eine klar konturierte Rechtsprechung zu einer solchen Informationshaftung gibt es allerdings nicht.

Dementsprechend blieb die Regelung zur Datenqualität ein mit wenig Leben gefülltes Relikt. Zu Recht betonte daher eine Expertenkomission der US-Regierung schon 1977: „The Commission relies on the incentives of the marketplace to prompt reconsideration of a rejection if it turns out to have been made on the basis of inaccurate or otherwise defective information".[10]

Der Markt und damit auch das allgemeine Zivilrecht sollten demnach über das Versagen der Unternehmen bei der Verwendung veralteter oder unrichtiger Daten entscheiden.

II. Die Vorgeschichte hin zur Datenqualität[11]

1. Das Mutterland: Die USA

Erstaunlicherweise stammt der Grundsatz der Datenqualität aus den USA, eigentlich einem der Länder, dem ein europäischer Datenschützer das wohl eher nicht zugetraut hätte. Der noch heute geltende US Privacy Act 1974[12] enthält zahlreiche Anforderungen an eine Datenverarbeitung im Hinblick auf die „accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness".[13]

Die Regelung bezieht sich allerdings nur auf die Verarbeitung personenbezogener Daten durch den Staat („Agencies") und sicherte dem Be-

---

[10] Epic.org, Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, https://epic.org/privacy/ppsc1977report/c1.htm (zuletzt abgerufen am 24.08.2016).

[11] Spätestens hier zeigt sich, dass es ein wichtiges Desiderat der Rechtsgeschichte bleibt, die Geschichte des Datenschutzrechts aufzuarbeiten. Ansätze dazu bei *Büllesbach/Garstka*, CR 2005, 720 ff. ; *v. Lewinski*, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt et al., Freiheit – Sicherheit – Öffentlichkeit, 2009, S. 196 ff.

[12] http://www.archives.gov/about/laws/privacy-act-1974.html (zuletzt abgerufen am 24.08.2016).

[13] 5 U.S.C. 552 a (e) (5) betreffend die Datenverarbeitung staatlicher "agencies".

troffenen über die Gewährleistung der Datenqualität einen fairen Entscheidungsprozess der Behörde.

In den USA wurde im Übrigen 2001 als Bestandteil des Consolidated Appropriations Act der Data Quality Act (DQA), auch Information Quality Act genannt (IQA), verabschiedet. Er ermächtigt das Office of Management and Budget dazu, Richtlinien zu erlassen, welche die Qualität und Integrität von Informationen sicherstellen und erhöhen sollen, die durch staatliche Einrichtungen veröffentlicht werden („Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies“[14]).[15] Darüber hinaus sollen Mechanismen geschaffen werden, die es den von der Verbreitung fehlerhafter Informationen Betroffenen ermöglichen, dies anzuzeigen und korrigieren zu lassen.[16]

Eine Differenzierung zwischen personenbezogenen und nichtpersonenbezogenen Daten wird hierbei allerdings nicht vorgenommen. Hinzu kommt, dass der Anwendungsbereich des Data Quality Act sich in der Verbreitung von Informationen durch staatliche Behörden gegenüber der Öffentlichkeit erschöpft.[17]

Darüber hinaus gibt es kein bundeseinheitliches Gesetz, das Vorgaben für die Datenqualität von personenbezogenen Daten für den nichtstaatlichen Bereich aufstellt. Da das US-amerikanische Datenschutzrecht durch zahlreiche Gesetze und Leitlinien auf Bundes- und Staatenebene geregelt ist, gibt es vereinzelt bereichsspezifische Gesetze, die Regelungen zur Datenqualität enthalten (z.B. der Fair Credit Reporting Act oder der Health Insurance Portability and Accountability Act of 1996). Beispielsweise verpflichtet der Fair Credit Reporting Act Nutzer von Verbraucherberichten, Verbraucher über ihr Recht aufzuklären, die Richtigkeit der sie betreffenden Berichte zu bestreiten. Ein weiteres Beispiel ist die HIPAA Security Rule, wonach betroffene Einrichtungen (z.B. Gesundheitspro-

---

[14] White House, Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies, https://www.whitehouse.gov/omb/fedreg_final_information_quality_guidelines/ (zuletzt abgerufen am 24.08.2016).

[15] https://www.whitehouse.gov/omb/fedreg_reproducible (zuletzt abgerufen am 24.08.2016).

[16] Subsection (2) (B) of the DQA.

[17] *Wait/Maney*, Environmental Claims Journal, 145 (148).

gramme, Abrechnungsstellen für Gesundheitsversorgung oder Gesundheitsversorgungsunternehmen) die Integrität von elektronisch geschützten Gesundheitsdaten sicherstellen müssen.[18]

2. Die OECD Guidelines 1980

Die US-Grundsätze wurden übernommen und ausgeweitet in den OECD-Guidelines 1980[19]. Dabei gilt es zu beachten, dass die Richtlinien von vornherein als nicht-verbindliche Empfehlungen konzipiert waren.[20] Guideline 8 enthält den allgemeinen Hinweis auf das Gebot der „Accuracy" der Daten. Zur Erläuterung wurde darauf hingewiesen: "Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept"[21] Noch detaillierter geregelt war die Frage der Datenqualität in einer zweiten OECD-Empfehlung aus dem Jahre 1980, den „15 Principles on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters".[22] Principle Nr. 5 enthielt detaillierte Ausführungen zur Datenqualität, die weit über den heutigen Stand hinausgingen.

> *"Personal data must be: (..) -accurate and, where necessary, kept up to date; 2. Personal data must be evaluated taking into account their degree of accuracy or reliability, their source, the categories of data subjects, the purposes for which they are processed and the phase in which they are used."*

---

[18] *Sotto/Simpson*, United States, in: Roberton, Data Protection & Privacy, S. 210 f.

[19] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (23 September 1980), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (zuletzt abgerufen am 24.08.2016). Dazu *Patrick*, Jurimetrics 1981, Vol. 21, No. 4, 405 (405 ff.).

[20] *Kirby*, International Data Privacy Law 2011, Vol. 1, No. 1, 6 (11), http://idpl.oxfordjournals.org/content/1/1/6.full.pdf (zuletzt abgerufen am 24.08.2016).

[21] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#comments (zuletzt abgerufen am 24.08.2016).

[22] http://www.statewatch.org/news/2007/may/oecd-1980s-data-protection-principles.pdf (zuletzt abgerufen am 24.08.2016).

Schon damals gab es Zweifel innerhalb der OCED-Expertengruppe, ob Datenqualität eine Kategorie des Datenschutzes ist:

> *"In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection."*[23]

So stritten sich auch externe Experten[24] um die Sinnhaftigkeit eines solchen Konzepts:

> *"Reasonable though that expression is, the use of a term which bears an uncertain relationship to the underlying discipline risks difficulties in using expert knowledge of information technology to interpret and apply the requirements."*[25]

Zu Recht wurde immer wieder betont, dass es sich um ein allgemeines Fachkonzept der Informatik handele:

> *"Data quality is a factor throughout the cycle of data collection, processing, storage, processing, internal use, external disclosure and on into further data systems. Data quality is not an absolute concept, but is relative to the particular use to which it is to be put. Data quality is also not a static concept, because data can decay in storage, as it becomes outdated, and loses its context. Organisations therefore need to take positive measures at all stages of data processing, to ensure the quality of their data. Their primary motivation for this is not to serve the privacy interests of the people concerned, but to ensure that their own decision-making is based on data of adequate quality."*[26]

---

[23] So steht es ausdrücklich in den Erläuterungen zu den Guidelines, Explanatory Memorandum, Rdnr. 53.

[24] Zur Expertengruppe der OCED siehe *Fuster*, The Emergence of Personal Data Protection as a Fundamental Right of the EU, S. 78 f.

[25] *Clarke*, The OCED Guidelines, http://www.rogerclarke.com/DV/PaperOECD.html (zuletzt abgerufen am 24.08.2016).

[26] *Clarke*, The OCED Guidelines, http://www.rogerclarke.com/DV/PaperOECD.html (zuletzt abgerufen am 24.08.2016).

3. Art. 6 der EU-Datenschutzrichtlinie und seine Auswirkungen in Kanada

Die damals schon weltweit anerkannten OECD-Standards wurden später in die EU-Datenschutzrichtlinie aufgenommen.[27] Im ersten Entwurf der Richtlinie[28] findet sich nur eine allgemeine Beschreibung der Erlaubnistatbestände für eine Datenverarbeitung der öffentlichen Hand.[29] Erst in Art. 16 findet sich die Pflicht, "accurate" personenbezogene Daten zu verarbeiten – ohne Bezug zur Frage der Zulässigkeit der Datenverarbeitung. In der zweiten Version von Oktober 1992[30] wurde diese Regelung dann zu Art. 6 des Textes und damit in die Nähe zur Zulässigkeit der Verarbeitung gerückt. Sanktionen waren nicht vorgesehen. Auch jetzt war noch die Verbindung der Datengrundsätze zur Zulässigkeit der Verarbeitung ungeklärt. Die Datengrundsätze behielten ihren Charakter als Programmsätze mit Empfehlungscharakter.

Länder wie Kanada schlossen sich unter dem Druck der EU mit dem PIPEDA Act im Jahre 2000 den dortigen Grundsätzen der Datenqualität an:

> *"Personal information shall be as accurate, complete and up to date as is necessary for the purposes for which it is to be used. The extent to which personal information shall be accurate, complete and up to date will depend upon the use of the information, taking into account the interests of the individual."*[31]

In sog. Guidelines wurde in Kanada der Grundsatz der „Accuracy" noch konkretisiert:

> *"Information shall be sufficiently accurate, complete and up to date to minimize the possibility that inappropriate information may be used to make a decision about the individual. An organization shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected. Per-*

---

[27] Dazu allgemein *Cate*, 80 Iowa Law Review 1995, 431 (431 ff.).

[28] Zu finden unter http://aei.pitt.edu/3768/1/3768.pdf (zuletzt abgerufen am 24.08.2016).

[29] KOM (90) 314 endg. SYN 287, S. 53.

[30] http://aei.pitt.edu/10375/ (zuletzt abgerufen am 24.08.2016).

[31] Personal Information Protection and Electronic Documents Act (PIPEDA), (S.C. 2000, c. 5). Dazu *Austin*, University of Toronto Law Journal 2006, 181 (181 ff.).

sonal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up to date, unless limits to the requirement for accuracy are clearly set out."[32]

Von den EU-Ländern erwies sich bei der Umsetzung der EU-Datengrundsätze vor allem Großbritannien als Pionier. In Großbritannien wurde die EU-Datenschutzrichtlinie mit dem Data Protection Act 1998 umgesetzt. Während der Data Protection Act 1998 die Grundzüge des britischen Datenschutzrechts regelt, erfolgt eine Konkretisierung dieser Vorschriften im Rahmen von Verordnungen (statutory instruments) und Rechtsvorschriften (regulations).[33] Der Data Protection Act 1998 stellt insgesamt acht Datenschutzprinzipien auf. Die Qualitätsregel des Artikel 6 Abs. 1 d) der EU-Datenschutzrichtlinie wurde im Rahmen des vierten Datenschutzprinzips umgesetzt, welches vorschreibt, dass personenbezogene Daten aktuell und sachlich richtig sein müssen.[34]

Aus Gründen der Praktikabilität trifft der Act Sonderregelungen für die Fälle, in denen Personen Informationen über sich selbst bereitstellen oder personenbezogene Daten von Dritten erlangt werden. Auch wenn in diesen Fällen personenbezogene Daten sachlich falsch sind, wird dies nicht als Verstoß gegen das vierte Datenschutzprinzip angesehen, wenn beim Betroffenen oder einem Dritten falsche Informationen korrekt erfasst wurden, der Verantwortliche angemessene Maßnahmen („reasonable steps") zur Sicherung der Datenqualität getroffen hat und die Daten erkennen lassen, dass der Betroffene den Verantwortlichen auf die Ungenauigkeiten hingewiesen hat.[35]

---

[32] Sect. 4.6. der Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96. Siehe dazu auch *Scassa/Deturbide,* S. 135 ff.

[33] Taylor Wessing, An overview of UK data protection law, http://united-kingdom.taylorwessing.com/uploads/tx_siruplawyermanagement/NB_000168_Overview_UK_data_protection_law_WEB.pdf (zuletzt abgerufen am 24.08.2016).

[34] Sch. 1 Pt. 1 Para. 4 Data Protection Act 1998; ausführliche Informationen zum vierten Datenschutzprinzip unter https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/ (zuletzt abgerufen am 24.08.2016)

[35] Sch. 1 Pt. 2 Para. 7 Data Protection Act 1998.

Was genau unter angemessenen Maßnahmen zu verstehen ist, richtet sich nach der Art der personenbezogenen Daten und danach, welche Bedeutung die Korrektheit im Einzelfall hat.[36]

Im Jahr 2013 hob der UK Court of Appeal im Fall „Smeaton v Equifax Plc" hervor, dass der Data Protection Act 1998 keine absolute Verpflichtung zur Gewährleistung der Richtigkeit personenbezogener Daten begründe, sondern nur die Vornahme angemessener Maßnahmen verlange, welche die Datenqualität sicherstellen sollen. Die Angemessenheit ist nach dem jeweiligen Einzelfall zu beurteilen. Auch ergebe sich aus dem vierten Datenschutzprinzip keine parallele Verpflichtung auf dem Gebiet des Deliktsrechts.[37]

Trotz dieser internationalen Entwicklungen kurz vor der Jahrtausendwende blieb das Prinzip der Datenqualität allerdings nahezu unbeachtet, als „the most forgotten of all of the internationally recognized privacy principles".[38]

III. Die Datenqualität in der EU-DSGVO

Die Rechtsnatur der Datengrundsätze änderte sich erst mit der EU-DSGVO.

1. Erstaunlich: Art. 5 als Grundlage von Bußgeldern

Am Anfang hatte die VO noch das Ziel, die Grundsätze aus der EU-Datenschutzrichtlinie als Empfehlungen ohne Sanktionen nahezu wörtlich zu übernehmen.[39]

Irgendwann während der Trilog-Gespräche änderte sich jedoch offensichtlich die Haltung, ohne dass man die Akteure aus den ohnehin nicht

---

[36] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/ (zuletzt abgerufen am 24.08.2016).

[37] Smeaton v Equifax Plc [2013] ECWA Civ 108, http://www.bailii.org/ew/cases/EWCA/Civ/2013/108.html (zuletzt abgerufen am 24.08.2016).

[38] *Cline*, Data quality - the forgotten privacy principle, Computerworld-Online v. 18.09.2007, http://www.computerworld.com/article/2541015/security0/data-quality----the-forgotten-privacy-principle.html (zuletzt abgerufen am 24.08.2016).

[39] Siehe Art. 5 (1) (d) der Fassung vom 11.6.2015: „Personenbezogene Daten müssen (d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein."

veröffentlichten Trilog-Papieren identifizieren könnte. Jedenfalls tauchte im Trilog-Kompromisspapier von Dezember 2015 auf einmal der Hinweis auf, dass auch die Datenschutzgrundsätze mit dem höchsten Level der Bußgeldsanktionen versehen werden (Art. 83 (5) (a)). Seitdem ist auch der Grundsatz der Datenqualität seinem Status als reiner Programmsatz entronnen und gilt nunmehr auch als ein ordnungswidrigkeitsrechtlicher Bußgeldtatbestand. Diese von der Öffentlichkeit kaum beachtete Veränderung ist fatal und schwierig, wie im Weiteren zu zeigen sein wird.

Fraglich ist zum Beispiel, ob tatsächlich ein Bußgeld in Höhe von maximal 4% des Jahresumsatzes bei Verletzung der Qualitätsregel verhängt werden könnte. Denn das Kriterium der „sachlichen Richtigkeit" ist unklar. Was bedeutet „sachlich"? Dem Begriff liegt eine duale Kategorisierung mit „richtig" und „unrichtig" zugrunde. Sie basiert auch auf der alten, schon bei § 35 BDSG diskutierten Abgrenzung zwischen Tatsachen und Meinungen.[40] Tatsachenbehauptungen können „richtig" oder „unrichtig" sein, nicht aber Werturteile. Ist „richtig" identisch mit „wahr"? Der englische Text der VO spricht nicht von „richtig", sondern von „accurate".

Dieser Terminus ist vielschichtiger als die deutsche Übersetzung. Er umfasst die Zielgerichtetheit, Genauigkeit, Exaktheit im Sinne der Mathematik. Er stammt aus der Ingenieurwissenschaft und der frühen Informatik und findet sich aus dieser Wurzel heraus als Zentraldefinition in modernen ISO-Normen.[41] Er findet sich in diesem Sinne auch in den oben erwähnten Spezialregelungen für Statistikbehörden oder Luftfahrtorganisationen. Der Terminus war insofern auch nie im ontologischen Sinne gemeint und damit auch nicht auf die bipolare Beziehung von „richtig" und „unrichtig" bezogen. Gemeint war der Begriff traditionell eher relational auf „eher akkurat". Für den Ordnungswidrigkeitentatbestand ist der Begriff nach Art. 103 II GG eindeutig zu unbestimmt.[42] Zugleich besteht die Gefahr, dass die Datenschutzaufsicht zur Megabehörde für richtige Daten mutiert, vor allem im Lichte des weiten Begriffs des Personenbezugs in Art. 4 Abs. 1 der VO. Die Datenschutz-Aufsichtsbehörde ist gar nicht in

---

[40] Siehe dazu *Mallmann*, in: Simitis, BDSG, § 20 Rdnr. 17 ff.; *Dix*, in: Simitis, BDSG, § 35 Rdnr. 13.

[41] ISO 5725-1:1994.

[42] BVerfGE 75, 329 (341).

der Lage, die mathematisch-statistische Validität von Datenverfahren zu beurteilen. Dies war auch bislang nie ihre Aufgabe und ihre Kernkompetenz. Die Datenschutzaufsichtsbehörde müsste dann selbständig mit Hilfe eingestellter Mathematiker die Validität überprüfen.

2. Verhältnis zu den Betroffenenrechten

Zu beachten ist auch, dass die VO selbst eigene Verfahrensinstrumente zugunsten des Betroffenen und der Sicherung der in seinem Sinne richtigen Daten vorsieht. Nach Art. 16 hat der Betroffene einen Anspruch auf Richtigstellung („Rectification") bei „inaccurate personal data". Art. 18 ergänzt den Schutz des Betroffenen durch das Recht auf Beschränkung der Verarbeitung in Fällen, in denen die Richtigkeit der Daten vom Betroffenen bestritten wird; auf einen solchen Widerspruch hat der Datenverarbeiter die Möglichkeit, die Richtigkeit der Daten zu überprüfen. Art. 16 und 18 greifen mit „inaccurate" bzw. „accuracy" die Formulierung aus Art. 5 bewusst auf und korrespondieren insofern mit dem Gebot der Datenrichtigkeit. Die Vorschriften zeigen auch, dass sich Art. 5 nicht darin erschöpft, zugunsten des Betroffenen die zu seinen Gunsten richtigen Daten zu sichern. Art. 83 Abs. 5 b) sanktioniert die Einhaltung der Betroffenenrechte ebenfalls mit der höchsten Bußgeldstufe. Allerdings meint „Accuracy" hier „Richtigkeit" im obigen Sinne. Es gilt, eine Vermengung zweier Konzepte in der VO interpretatorisch zu vermeiden: den technologisch-relationalen Begriff der „Accuracy" mit der ontologisch-bipolaren Thematik der „Richtigkeit" von Behauptungen über den Betroffenen. Das Richtigkeitskonzept der Art. 12, 16 EUDSGVO hat nichts mit dem Accuracy-Modell von Art. 5 DSGVO zu tun. Deshalb ist es auch gefährlich, die Begriffe in Art 5 und Art. 12, 16 der VO identisch zu interpretieren.

3. Verhältnis Datenqualität und Zulässigkeit der DV

Auch ist unklar, wie sich die Beziehung von Art. 5 und 6 EU-DSGVO gestaltet. Zunächst einmal fragt sich, ob nicht das Gebot der Datenrichtigkeit zu einem Erlaubnistatbestand im Sinne von Art. 6 lit. f DSGVO genutzt werden kann. Ein legitimes Interesse für die Datenverarbeitung wäre dann die Tatsache, dass die Daten nach Art. 5 immer „up-to-date" gehalten werden müssen.

4. Art. 5 als abstraktes Gefährdungsdelikt?

Denkbar wäre eine restriktive Auslegung von Art. 5 oder die Einordnung als abstraktes Gefährdungsdelikt.[43] Die oben genannte Einstiegsfrage kommt einem wieder in den Kopf: Müsste man nicht Art. 5 teleologisch reduzieren und darauf beschränken, die Datenrichtigkeit nur dann einzufordern, wenn die Nichteinhaltung zu Lasten des Betroffenen geht? In diesem Sinne hat eine australische Juristenkommission[44] entsprechende Regelungen im australischen Datenschutzrecht verstanden: *"In the OPC Review, the OPC stated that it is not reasonable to take steps to ensure data accuracy where this has no privacy benefit for the individual."*

Ähnliche Korrekturansätze finden sich in der oben genannten britischen Rechtsprechung. Allerdings sprechen die allgemeine Gefahrenquelle und die erhöhten Risiken, die von großen Datenpools im Zeitalter von Big Data ausgehen, für das Vorliegen eines Gefährdungstatbestands. Auf solche Gefahrenlagen weisen auch ausländische Gerichte hin, darunter der kanadische Federal Court Ottawa; ausgerechnet aus dem Staat, der sich am weitesten in Sachen Datenqualität im Datenschutzrecht nach vorne gewagt hat. So hat der Federal Court in der Entscheidung „Nammo"[45] betont:

> *"An organization's obligations to assess the accuracy, completeness and currency of personal information used is an ongoing obligation; it is not triggered only once the organization is notified by individuals that their personal information is no longer accurate, complete or current. Responsibility for monitoring and maintaining accurate records cannot be shifted from organizations to individuals."*

---

[43] *Anastasopoulou,* Deliktstypen zum Schutz kollektiver Rechtsgüter, S. 63 ff.; *Graul,* Abstrakte Gefährdungsdelikte und Präsumptionen im Strafrecht, S. 144 ff.; *Gallas,* Abstrakte und konkrete Gefährdung, in: Lüttger et al., Festschrift für Ernst Heinitz zum 70. Geburtstag, S. 171.

[44] Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice (ALRC Report 108), http://www.alrc.gov.au/publications/27.%20Data%20Quality/balancing-data-quality-and-other-privacy-interests (zuletzt abgerufen am 24.08.2016).

[45] Nammo v. TransUnion of Canada Inc., 2010 FC 1284: siehe http://www.fasken.com/files/upload/Nammo_v_Transunion_2010_FC_1284.pdf (zuletzt abgerufen am 24.08.2016).

Und die Datenschutzaufsicht in Ottawa betont in seinem Tätigkeitsbericht 2011[46]:

> *"By presenting potentially outdated or incomplete information from a severed data source, a credit bureau could increase the possibility that inappropriate information is used to make a credit decision about an individual, contrary to the requirements of Principle 4.6.1."*

M. E. sind beide Gedanken zu verbinden. Art. 5 d) ist die Grundlage eines abstrakten Gefährdungsdelikts und gerade deshalb restriktiv auszulegen. Dies gilt umso mehr, als Art 5 d) nunmehr nach Art. 83 Abs. 5 a) auch Grundlage eines Ordnungswidrigkeitenverfahrens mit massiven Bußgeldern sein kann. Allerdings kann und darf die restriktive Auslegung nicht dazu führen, dass aus einem abstrakten Gefährdungsdelikt ein konkretes wird. Dies würde den Wortlaut von Art. 5 d) der EU-DSGVO konterkarieren. Eine Auslegung, die weitreichende Auslegungseingriffe bei einem gerade verabschiedeten Verordnungstext vornimmt, ist m. E. vorläufig erst einmal zu vermeiden. Insofern ist Art. 5 d) im Ergebnis als abstrakter Gefährdungstatbestand und damit weit auszulegen. Die korrespondierende Regelung im neuen Bußgeldtatbestand gilt es jedoch eng und behutsam einzusetzen.

IV. Fazit und Ausblick

Das Beispiel der ausländischen Regelungen, etwa in den USA und Kanada, sowie der Weg von der EU-Datenschutzrichtlinie zur EU-DSGVO zeigen, dass die steigende Relevanz des Themas Datenqualität immer mehr erkannt wird. Allerdings kann „Veracity"[47] bzw. „Accuracy" von

---

[46] Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2011-009, https://www.priv.gc.ca/cf-dc/2011/2011_009_1122_e.asp (zuletzt abgerufen am 24.08.2016). Ähnlich bereits Office of the Privacy Commissioner of Canada , PIPEDA Case Summary #2003-224, https://www.priv.gc.ca/cf-dc/2003/cf-dc_031007_e.asp (zuletzt abgerufen am 24.08.2016); Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2003-163, https://www.priv.gc.ca/cf-dc/2003/cf-dc_030417_2_e.asp (zuletzt abgerufen am 24.08.2016).

[47] Siehe Übersicht zu den "Four V's of Big Data" (Volume, Variety, Velocity und Veracity), *Mohanty*, The Four Essential V´S for a Big Data Analystics Platform, Dataconomy-Online, http://dataconomy.com/the-four-essentials-vs-for-a-big-data-analytics-platform/ (zuletzt abgerufen am 24.08.2016).

Daten nur dann erreicht werden, wenn wirksame Instrumentarien geschaffen werden, die Qualitätsstandards für Daten gewährleisten können. Sowohl die EU-Richtlinie als auch der Data Quality Act stellen einen Weg in die richtige Richtung dar. Allerdings wird der bloße Verweis auf die Einhaltung von Qualitätsstandards nicht per se ausreichen, um Art. 5 der EU-DSGVO einzuhalten. Erinnert sei an den oben bereits mehrfach rezitierten kanadischen Nammo-Fall[48]:

> *"The suggestion that a breach may be found only if an organization's accuracy practices fall below industry standards is untenable. The logical conclusion of this interpretation is that if the practices of an entire industry are counter to the Principles laid out in Schedule I, then there is no breach of PIPEDA. This interpretation would effectively deprive Canadians of the ability to challenge industry standards as violating PIPEDA."*

Diese Warnung ist besonders deshalb wichtig, weil es im Bereich der Datenqualität keine weltweit gültigen und anerkannten Industriestandards gibt. Von einer Harmonisierung und echten Standardisierung sind wir noch weit entfernt. Insofern sollten die Datenschutzaufsichtsbehörden den neu eingeschrittenen Weg der strafrechtlichen Sanktionierung von Datenqualität sehr behutsam und mit Augenmaß beschreiten.

Literaturnachweise

Anastasopoulou, Deliktstypen zum Schutz kollektiver Rechtsgüter, München 2005.

Austin, Is Consent the Foundation of Fair Information Practices? Canada's Experience under Pipeda, The University of Toronto Law Journal 2006, Vol. 56, No. 2, 181-215.

Büllesbach/Garstka, Meilensteine auf dem Weg zu einer datenschutzgerechten Gesellschaft, CR 2005, 720-724.

Cate, 80 Iowa Law Review 1995, 431-443.

Clarke, The OECD Data Protection Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law, Canberra 1989.

[48] Nammo v. TransUnion of Canada Inc., 2010 FC 1284.

Cline, Data quality - the forgotten privacy principle, Computerworld-Online, http://www.computerworld.com/article/2541015/security0/data-quality----the-forgotten-privacy-principle.html (zuletzt abgerufen am 24.08.2016).

Derleder, Das Milliardengrab - Ein bemerkenswertes Urteil offenbart pikante Details in der Causa Kirch gegen Deutsche Bank, NJW 2013, 1786-1789.

Fuster, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Cham 2014.

Gallas, Abstrakte und konkrete Gefährdung, in: Lüttger et al. (Hrsg.), Festschrift für Ernst Heinitz zum 70. Geburtstag, Berlin 1972, S. 171-184.

Graul, Abstrakte Gefährdungsdelikte und Präsumptionen im Strafrecht, Berlin 1989.

Höpfner/Seibl, Bankvertragliche Loyalitätspflicht und Haftung für kreditschädigende Äußerungen nach dem Kirch-Urteil, BB 2006, 673-679.

Kirby, The history, achievement and future of the 1980 OECD guidelines on privacy, International Data Privacy Law 2011, Vol. 1, No. 1, 6-14.

v. Lewinski, Geschichte des Datenschutzrechts von 1600 bis 1977, in: von Arndt et al. (Hrsg.): Freiheit – Sicherheit – Öffentlichkeit, Heidelberg 2008, S. 196-220.

Mohanty, The Four Essential V´S for a Big Data Analystics Platform, Dataconomy-Online, http://dataconomy.com/the-four-essentials-vs-for-a-big-data-analytics-platform/ (zuletzt abgerufen am 24.08.2016).

Patrick, Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines, Jurimetrics Vol. 21, No. 4 1981, 405-420.

Simitis, Kommentar zum Bundesdatenschutzgesetz, 8. Aufl. Baden-Baden 2014.

Sotto/Simpson, United States, in: Roberton (Hrsg.), Data Protection & Privacy 2015. London 2014, S. 208-214.

Scassa/Deturbide, Electronic Commerce and Internet Law in Canada, 2. Aufl. Toronto 2012.

Wait/Maney, Regulatory Science and the Data Quality Act, in: Environmental Claims Journal 2006, S. 145-162.