www.jusletter-it.eu

Daniela Nüesch

Tagungsbericht zur achten schweizerischen Datenschutzrechtstagung zum Thema Big Data und Datenschutzrecht

The eighth Swiss conference regarding data protection of 28-29 May 2015 focused on «Big Data and Data Protection». In particular, numerous questions in this context were examined from interdisciplinary points of view and multiple perspectives. To reflect the current state of research in its main features and to roughly indicate the dealing with the problem in the legal praxis, the author summarises the particular presentations and ateliers and makes a note of the consequent possible actions. (ah)

Category: Conference Proceedings
Region: Switzerland
Field of law: Data Protection

Citation: Daniela Nüesch, Tagungsbericht zur achten schweizerischen Datenschutzrechtstagung zum Thema Big Data und Datenschutzrecht, in: Jusletter IT 24 September 2015

Inhaltsübersicht

I. Einleitung

[Rz 1] Dass Amazon ermitteln kann, welche konkreten Filme eine Person mögen könnte, dass ein Supermarkt herauszufinden vermag, ob eine seiner Kundinnen schwanger ist und dass Epidemien oder auch deliktisches Verhalten vorhergesagt werden können, lässt sich auf einen gemeinsamen Nenner zurückführen. Beispielshaft angedeutet werden damit die technischen Möglichkeiten in Zusammenhang mit *Big Data*, die in allerlei Branchen bereits zum Zuge kommen bzw. zukünftig herangezogen werden könnten.[1] Der Begriff *Big Data* bezieht sich dabei nicht nur – wie bereits aus seinem Wortlaut erkennbar – auf eine grosse Menge von aus verschiedenen Quellen stammenden Daten, sondern bezeichnet gleichzeitig die Nutzung dieser Daten mittels leistungsfähiger Analysetools, um daraus neue Erkenntnisse zu gewinnen.[2] Mit *Big Data* zeichnet sich somit eine neue Form des Umgangs mit Informationen ab, welche die derzeit bestehenden datenschutzrechtlichen Regelungen vor grundlegende Herausforderungen stellt. Die damit zusammenhängenden rechtlichen Fragestellungen wurden an der diesjährigen schweizerischen Datenschutzrechtstagung unter Mitberücksichtigung weiterer Aspekte – soziologischer oder auch technischer Natur – eingehend diskutiert. Im Verlaufe dieses Jahres wird zudem ein Tagungsband erscheinen, der die schriftliche Fassung der an der Datenschutzrechtstagung gehaltenen Referate enthält.

[Rz 2] Der Aufbau des folgenden Beitrags schliesst an den Ablauf der Tagung an und bezieht sich zunächst auf die Referate zu grundlegenden Fragestellungen im Bereich *Big Data* und Da-

---

1 Für weitere Anwendungsbeispiele s. Astrid Epiney, Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf, in: Jusletter IT 21. Mai 2015, Rz. 2.

2 Epiney (Fn. 2), Rz. 5f.; siehe auch die Begriffsumschreibung von Bitkom, Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte, 2012, 7ff., einsehbar unter https://www.bitkom.org/Publikationen/2012/Leitfaden/Leitfaden-Big-Data-im-Praxiseinsatz_Szenarien_Beispiele_Effekte/BITKOM_LF_big_data_2012_online%281%29.pdf (alle Internetquellen zuletzt besucht am 29. Juli 2015) und Rolf H. Weber, Big Data: Rechtliche Perspektive, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 17 (17ff.) sowie weitere Definitionsansätze, die *Big Data* anhand der sie kennzeichnenden «Vs» (*volume*, *velocity*, *variety*, *veracity* und *value*) umschreiben, so z.B. http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=de oder auch Andreas Wespi, Big Data: Technische Perspektive, in: Rolf H. Weber/Florent Thouvenin (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 3 (4f.).

tenschutzrecht (II.), während im darauffolgenden Teil die einzelnen Ateliers zu spezifischen Problemstellungen im Bereich des Datenschutzrechts (III.) dargestellt werden. Der Beitrag endet mit einigen abschliessenden Bemerkungen (IV.).

II. Referate zu grundlegenden Fragestellungen im Bereich Big Data und Datenschutzrecht

1. Big Data: Herausforderungen für das Datenschutzrecht

[Rz 3] Im Eröffnungsvortrag erörterte Prof. Dr. Rolf H. Weber die Potenziale und Risiken von *Big Data* sowie die sich daraus ergebenden Problemstellungen im Kontext des geltenden Datenschutzrechts, wobei mögliche Lösungsansätze sowie zukünftige Entwicklungen im Zentrum seines Referats standen. *Big Data*-Analysen liefern seiner Meinung nach zwar sachdienliche Entscheidungsgrundlagen – die insbesondere auch unter wirtschaftlichen Gesichtspunkten von grossem Nutzen sind, sie führen aber aufgrund der auf Wahrscheinlichkeiten beruhenden Analysemethoden nicht zwangsläufig zu richtigen Ergebnissen. Dazu kommt, dass die Beurteilung der Anwendbarkeit der datenschutzrechtlichen Bestimmungen im Fall von *Big Data*-Anwendungen erhebliche Schwierigkeiten bereitet. Denn *Big Data* bringt mit sich, dass ursprünglich anonymisierte Daten, die vom Anwendungsbereich des Datenschutzgesetzes nicht erfasst sind, in Verbindung mit weiteren Daten de-anonymisiert werden und damit zu einem späteren Zeitpunkt datenschutzrechtlich relevant werden können. Des Weiteren ging der Referent der Frage nach, wie mit dem Widerspruch von *Big Data* mit den allgemeinen Datenschutzgrundsätzen, wie etwa dem Zweckbindungsprinzip, dem Prinzip der Transparenz, der Datenminimierung sowie der Richtigkeit der Daten, umzugehen ist. Namentlich gilt es gemäss dem Referenten die Geeignetheit des Konzepts der Einwilligung als Rechtfertigungsgrund für eine Persönlichkeitsverletzung zu überdenken. Denkbar wäre stattdessen die Implementierung der sog. *Accountability*, welche den Unternehmen zum Zweck der besseren Einhaltung der datenschutzrechtlichen Vorgaben Rahmenbedingungen in einer Mischform zwischen Selbstregulierung und staatlicher Regulierung setzt. Alternativ dazu sei auch die Einführung von Beteiligungsmodellen, bei welchen die Unternehmen und die betroffenen Personen auf der Grundlage von Mitbenutzungsrechten gemeinsam am Wert der Daten teilhaben, ein möglicher Lösungsansatz, um den aufgezeigten Problemstellungen zu begegnen. Besonders hervorzuheben ist schliesslich die Anregung des Referenten, den Fokus auf das Alternativkonzept *Smart Data* zu richten, welches impliziert, dass nur diejenigen Daten gesammelt werden, die auch tatsächlich einen Mehrwert erzeugen. Auf diese Weise liesse sich das Konfliktpotenzial zu den datenschutzrechtlichen Vorgaben möglicherweise wesentlich reduzieren.

2. Big Data und der Schutz der Privatsphäre

[Rz 4] Das Referat des Soziologen Dr. Sami Coll widmete sich dem Bedeutungsgehalt von *Big Data* und den damit einhergehenden Auswirkungen auf die gegenwärtige Informationsgesellschaft. Zur Begriffsbestimmung von *Big Data* knüpfte der Referent an die Massenspeicherung von Daten in nicht strukturierten Datenbeständen an. Die darin gespeicherten Daten können durch den Einsatz von Algorithmen als Mittel für eine möglichst umfassende Datenanalyse (möglicherweise gar in Echtzeit) beispielsweise für Vorhersagen genutzt werden. Als weiteres Charakteristikum wurde erwähnt, dass die gesammelten Daten oftmals zu Zwecken verwendet werden, die bei der Beschaf-

fung nicht angegeben worden sind. Darüber hinaus zeichnet sich *Big Data* dadurch aus, dass die in den verschiedenen Datenbanken gespeicherten Daten miteinander verknüpft werden können. Auch wenn *Big Data* der Forschung verheissungsvolle Möglichkeiten eröffnet, seien die mit *Big Data* einhergehenden «sozialen Sünden» nicht zu verkennen. Diesbezüglich machte der Referent als erstes darauf aufmerksam, dass mit *Big Data* nur eine bestimmte – neben den herkömmlichen Wissensquellen bestehende – Weise der Erlangung neuer Erkenntnisse gemeint ist. Die Eigenheit von *Big Data* bestehe dabei insbesondere darin, dass sich die daraus gewonnenen Erkenntnisse auf Wahrscheinlichkeiten und nicht auf Kausalitäten stützen und infolgedessen zu falschen Schlüssen führen können. Zweitens habe *Big Data* zur Folge, dass gewissen (neuen) Akteuren eine gewichtige Entscheidungsbefugnis beispielsweise zum Zweck der Vorbeugung von Krankheiten oder zur Gewinnmaximierung zukomme, wobei deren demokratische Legitimität hinterfragt werden müsse. Schliesslich äusserte der Referent Zweifel an der Schutzwirkung des ursprünglich freiheitlich ausgerichteten Konzepts der Privatsphäre. Der Grund sei namentlich darin zu sehen, dass sich die normativ-rechtliche Auffassung der Privatsphäre nicht mit den Vorstellungen und täglichen Erfahrungen des Einzelnen decke. Dem staatlichen Schutz der Privatsphäre liege das Recht auf informationelle Selbstbestimmung zugrunde, das nach Auffassung des Referenten einen zu individualistischen Ansatz verfolge und dementsprechend kollektiven Werten nicht genügend Rechnung trage. Dadurch sei, so die abschliessende Überlegung des Referenten, vielmehr einem im Interesse der Unternehmen und des Staates stehenden Informationskapitalismus gedient.

3. Big Data und Datenschutzrecht in Europa

[Rz 5] Der bayerische Landesbeauftragte für Datenschutz, Dr. jur. Thomas Petri, legte in seinem Referat den Fokus auf die europarechtliche Beurteilung der Problematik von *Big Data*. Ausgangspunkt bildete hierbei die Bestimmung des Begriffs von *Big Data*, welcher sich aus Sicht des Referenten auf eine geistige Haltung bezieht, die auf maximalen Erkenntnisgewinn zielt. Um das Spannungsverhältnis von *Big Data* zum geltenden Datenschutzrecht aufzuzeigen, gab der Referent zunächst einen Überblick über die relevanten Rechtserlasse auf internationaler, regionaler und nationaler Ebene. Dies führte den Referenten nachfolgend dazu, die einzelnen Konfliktpunkte von *Big Data* mit den zentralen Regelungen des Datenschutzrechts, namentlich dem Grundsatz von Treu und Glauben, dem Zweckbindungsprinzip, dem Prinzip der Datensparsamkeit, dem Schutz besonders sensitiver Daten sowie der Wahrung der Betroffenenrechte, deutlich zu machen. Die Einhaltung des Grundsatzes von Treu und Glauben und der Transparenz sowie die Wahrung der Betroffenenrechte setzten im Allgmeinen voraus, dass die Betroffenen in den Verarbeitungsprozess miteinbezogen werden. Dies dürfte im Rahmen von *Big Data* oftmals nicht der Fall sein, da bei solchen Anwendungen automatische und systematische Datenverarbeitungsmechanismen zum Zuge kommen. Ausserdem trete die Natur besonders schützenswerter Daten möglicherweise erst während des Auswertungsprozesses zum Vorschein, weshalb der Schutz solcher Daten zum Zeitpunkt ihrer Beschaffung nicht gewährleistet werden kann. Entgegen dem Zweckbindungsprinzip und dem Prinzip der Datensparsamkeit werde mit *Big Data* darüber hinaus eine möglichst grosse Menge an Daten unter anderem auch zu bei der Erhebung noch nicht vorhersehbaren Zwecken nutzbar gemacht. Diese Widersprüche dürften sich laut dem Referenten auch mit der neuen Datenschutzgrundverordnung, die zurzeit – nach der am 14. März 2014 abgeschlossenen ersten Lesung des Europäischen Parlaments und des Ratsbeschlusses vom 15. Juni 2015 – in Trilog-Verhandlungen zwischen den EU-Gesetzgebungsorganen verhandelt wird, nicht vollends auflösen. Denn auch wenn

die endgültige Fassung des neuen Rechtsrahmens noch nicht feststeht, ist aus Sicht des Referenten zu erwarten, dass die mit *Big Data* im Widerspruch stehenden Prinzipien in ihren Grundzügen erhalten bleiben. *Big Data* im Sinne eines uneingeschränkten Umgangs mit Personendaten werde deshalb auch in absehbarer Zeit nicht rechtlich zulässig sein.

4. Herausforderungen von Big Data für die Rechtsbeziehungen unter Privaten

[Rz 6] Im Rahmen seines Referats setzte sich Prof. Dr. Philippe Meier eingehend mit den Herausforderungen von *Big Data* in privatrechtlichen Beziehungen auseinander. Nach einer kurzen Einleitung in die Thematik und der Begriffsdefinition von *Big Data* befasste sich der Referent zunächst mit den grundlegenden datenschutzrechtlichen Fragestellungen, die sich aufgrund von *Big Data* im Bereich des Privatrechts stellen. Diesbezüglich kam der Referent nicht nur auf die Abgrenzung zwischen Personen- und Sachdaten sowie zwischen Personendaten und anonymisierten Daten zu sprechen, sondern er vertiefte in der Folge auch das Spannungsverhältnis von *Big Data* zu den verschiedenen datenschutzrechtlich verankerten Grundsätzen, namentlich der Verhältnismässigkeit, der Zweckbindung, der Erkennbarkeit und dem guten Glauben. Ausserdem wurde in diesem Zusammenhang ebenfalls die Frage nach der Legitimität und Effektivität des heutigen Einwilligungskonzepts aufgeworfen. *Big Data*-Anwendungen zu unterbinden hält der Referent nicht für angezeigt, vielmehr zieht er eine Reihe möglicher «interner» Lösungen in Betracht: den Anwendungsbereich des DSG auf alle Art Daten auszuweiten, zeitliche Aufbewahrungsgrenzen festzusetzen, alle mit dem ursprünglichen Zweck nicht unvereinbaren Datenbearbeitungen zuzulassen, die Verpflichtungen auf den Zeitpunkt der Wiederverwendung zu verschieben oder das System der Einwilligung durch eine bessere formelle Lesbarkeit zu stärken. Als weitere – nicht auf bestehenden datenschutzrechtlichen Instrumenten beruhende – Lösungsansätze wurden etwa die Monetarisierung der Daten bzw. der Nichtbeteiligung an *Big Data*, die Bildung von Nutzungsgemeinschaften verbunden mit verpflichtenden Vereinbarungen, die Betreuung der Daten als Allgemeingut durch eine zentrale Stelle, die Stärkung der Kontrollmechanismen sowie die Anpassung der Datenschutzbestimmungen in Hinblick auf die erleichterte Wahrnehmung der Rechte des Einzelnen angeführt. Dazu erwägt der Referent weitere Massnahmen, die sich sowohl auf einen verstärkten präventiven Schutz als auch auf eine ausgebaute nachträgliche Überprüfungsmöglichkeit beziehen. Neben den Auswirkungen von *Big Data* auf die Gesellschaft wird abschliessend zudem deren Stellenwert für die künftige Wissenschaftsforschung und Politik unterstrichen.

5. Big Data und der öffentliche Sektor

[Rz 7] Ergänzend zu den privatrechtlichen Ausführungen erörterte Prof. Dr. Markus Schefer die Bedeutung und Tragweite von *Big Data* im Bereich des öffentlichen Rechts. Anknüpfungspunkt und Grundlage seiner Erläuterungen bildete das Recht auf informationelle Selbstbestimmung, welches im Rahmen der bundesgerichtlichen Rechtsprechung aus dem in der Bundesverfassung gewährleisteten Recht auf Schutz vor Missbrauch der persönlichen Daten (Art. 13 Abs. 2 BV) abgeleitet wurde. Bezugnehmend auf *Big Data* ist der Schutzbereich des in Art. 13 Abs. 2 BV verankerten Grundrechts laut dem Referenten immer dann betroffen, wenn der Staat auf der Grundlage von berechneten Wahrscheinlichkeiten Handlungen gegenüber Privaten vollzieht. Die Anwendung von *Big Data* unterscheide sich dabei insofern von einer «gewöhnlichen» Datenbearbeitung, als sich aus

den im Rahmen von *Big Data* gewonnen Erkenntnissen korrelativ belegte Stereotypen ergeben, die auf die Gesellschaft zurückwirken und allenfalls zu Diskriminierungen führen können. Erschwerend kommt gemäss dem Referenten hinzu, dass der Einzelne von der in diesem Zusammenhang erfolgten Datenverarbeitung nicht notwendigerweise Kenntnis erhält und damit keine Möglichkeit hat, auf die Datenanalyse einzuwirken. Anders gestalte sich dies beispielsweise bei der Erstellung eines – wohl auf geringerer Wahrscheinlichkeit beruhenden – psychiatrischen Gutachtens, bei welchem die betroffene Person in den Datenverarbeitungsprozess miteinbezogen wird. Hinsichtlich einer besseren Bewältigung der mit *Big Data* zusammenhängenden Problematik legte der Referent besonderes Gewicht darauf, dass jede im Analyseverfahren zu erfolgende Datenverknüpfung gesondert zu beurteilen ist. Nur dadurch sei es möglich, den Interessen des Einzelnen im Rahmen einer Interessenabwägung genügend Rechnung zu tragen. Zusätzlich müssten die angewendeten Auswertungsmethoden den Betroffenen in einer für jedermann verständlichen Sprache dargelegt werden. Auf der Grundlage dieser Überlegungen brachte der Referent zum Schluss seine Bedenken in Bezug auf eine drohende Verengung des Grundrechts auf ein Recht auf Datenschutz zum Ausdruck.

6. Aktuelle Rechtsprechung im Bereich des Datenschutzes

[Rz 8] Bezugnehmend auf die Praxis der nationalen und kantonalen Gerichte stellte Prof. Dr. Alexandre Flückiger die aktuelle Rechtsprechung im Bereich des Datenschutzes vor. In Hinblick auf die in Art. 13 Abs. 2 BV normierte Verfassungsgrundlage stellte der Referent zunächst fest, dass sich die schweizerische Rechtsprechung bis auf Weiteres nicht eingehend mit der in der Lehre umstrittenen Frage nach dem Umfang des Schutzbereiches dieses Grundrechts auseinandergesetzt habe. Aus bundesgerichtlicher Rechtsprechung gehe jedoch klar hervor, dass sich das Recht auf informationelle Selbstbestimmung auf Art. 13 Abs. 2 BV stützen lässt und die erwähnte Rechtsgrundlage demzufolge nicht lediglich einen – wie die wörtliche Auslegung der Bestimmung nahelegen könnte – Schutz vor Missbrauch der Daten normiert. Grosse Beachtung in der gerichtlichen Praxis fand sodann die Durchsetzung des Auskunftsrechts. Diesbezüglich wurden zum einen verfahrenstechnische Fragen wie die Verteilung der Beweislast bei der Feststellung nicht vorhandener Personendaten geklärt und zum anderen über materiell-rechtliche Aspekte wie die Gewährleistung des indirekten Auskunftsrechts oder auch die Form des Datenzugangs befunden. Besondere Aufmerksamkeit erweckte dabei ein Fall,[3] in welchem eine Privatperson gestützt auf das Öffentlichkeitsgesetz des Kantons Genf detaillierte Angaben über ein dem Staat zugehöriges Gebäude verlangte. Abgelehnt wurde dieses Gesuch mit der Begründung, dass die Verwaltung von Immobilien durch den Kanton Genf aufgrund der Zuordnung des Gebäudes zum Finanzvermögen keine öffentliche Aufgabe im Sinne des Gesetzes über die Information der Öffentlichkeit und den Zugang zu Dokumenten des Kantons Genf (LIPAD)[4] darstelle und somit nicht von dessen Anwendungsbereich erfasst sei. Denn auch wenn die daraus generierten Einnahmen der Erfüllung staatlicher Aufgaben dienten, sei das Handeln des Staats laut Bundesgericht in einem solchen Fall mit demjenigen einer Privatperson gleichzusetzen. Aus diesem Grund sind die diesbezüglichen Informationen für die Öffentlichkeit nicht zugänglich. Nach einer kritischen Auseinandersetzung mit dem erwähnten Bundesgerichtsurteil befasste sich der Referent nicht nur mit weiteren datenschutzrechtlichen Aspekten wie der

3 Urteil des Bundesgerichts 1C_379/2014 vom 29. Januar 2015.

4 Loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001, RSG A 2 08.

Berichtigung personenbezogener Daten und der Anonymisierung von Urteilen und Verwaltungsentscheiden, sondern er diskutierte zum Schluss ebenfalls die sich in Einzelbereichen – insb. im Gebiet der Amtshilfe, des Arbeitsrechts und des Strafrechts – stellenden Problematiken.

III. Ausgewählte Problemstellungen in den Ateliers

1. Atelier I: Big Data in der Rechtspraxis – ausgewählte Problemstellungen

[Rz 9] Rechtsanwalt Roland Mathys illustrierte die Relevanz von *Big Data*-Anwendungen in der Rechtspraxis anhand einer anschaulichen Fallstudie, welche zusammen mit den Teilnehmenden erarbeitet wurde. Als Ausgangslage diente dabei die Fallkonstellation, in welcher ein Sportartikelhändler seine Kundenkarte durch ein smartes Armband zu ersetzen gedachte. Dies ermöglichte ihm, die mittels Armband gesammelten Daten – darunter Stammdaten, fitnessbezogene und einkaufsbezogene Daten sowie Geopositionsdaten – zu analysieren, auszuwerten und zur Erstellung von Persönlichkeitsprofilen miteinander zu verknüpfen, um schliesslich seine Kunden mit gezielter Werbung anzusprechen und die entsprechenden Daten gegebenenfalls an Dritte zu verkaufen. Ausgehend davon stellte sich in Anwendung der spezifisch dafür vorgesehenen AGB die Frage nach der rechtlichen Zulässigkeit der damit einhergehenden Datenbearbeitungen. Besonders eingehend diskutiert wurden dabei Fragen rund um das Vorliegen von Personendaten bzw. besonders schützenswerter Daten, die Einhaltung des Zweckbindungsgrundsatzes, die Zulässigkeit der Weitergabe der Daten an Dritte, die Risiken der Anonymisierung, die Berichtigung von auf Korrelationen beruhenden Daten, die Vorgaben bezüglich der Datenaufbewahrung und -löschung sowie die Rahmenbedingungen einer gültigen Einwilligung. Dabei konnten zahlreiche Fragenstellungen nicht abschliessend geklärt werden, womit der Referent zugleich deutlich machte, dass der Einsatz von *Big Data* auch mit zahlreichen praktischen Schwierigkeiten konfrontiert ist.

2. Atelier II: Rechtsprechung des EuGH zum Datenschutzrecht

[Rz 10] In seinem Atelier widmete sich Dr. iur. Markus Kern den Entwicklungen des Datenschutzrechts in der europäischen Rechtsprechung. Aufgegriffen wurde damit eine Thematik, die namentlich angesichts der im Rahmen der Schengen- und Dublin-Assoziierung bestehenden Übernahmepflichten auch für die Schweiz von zentraler Bedeutung ist. Das europäische Datenschutzrecht umfasst neben den im Primärrecht normierten Grundlagen zahlreiche, sekundärrechtlich geltende Regelungen, die bereichsspezifische Vorgaben festlegen. Mithin zeigt sich gemäss dem Referenten ein stark fragmentiertes EU-Rechtssystem im Bereich des Datenschutzes. Zur Veranschaulichung der EuGH-Rechtsprechung wurden drei *leading cases* herangezogen. Im Anschluss an die Urteile *Lindqvist*[5] und *Österreichischer Rundfunk*[6] befasste sich der Referent insbesondere mit der im Urteil *Google Spain*[7] aufgeworfenen Frage nach der Pflicht eines Suchmaschinenbetreibers, eine Verlinkung auf von Dritten zur Verfügung gestellte Inhalte zu entfernen. Im Rahmen dieses Vor-

5 Urteil des EuGH, Rs. C-101/01 vom 6. November 2003, ECLI: EU:C:2003:596 (*Lindqvist*).

6 Urteil des EuGH, verb. Rs. C-465/00, C-138/01 und C-139/01 vom 20. Mai 2003, ECLI:EU:C:2003:294 (*Österreichischer Rundfunk*).

7 Urteil des EuGH, Rs. C-131/12 vom 13. Mai 2014, ECLI:EU:C:2014:317 (*Google Spain*).

abentscheidungsverfahrens hielt der EuGH bezüglich der Tragweite des Löschungs- bzw. Widerspruchsrechts schliesslich fest, dass ein solches immer dann bestehe, wenn Daten nicht dem Verarbeitungszweck entsprechen, darüber hinausgehen oder zu deren Erfüllung nicht (mehr) erforderlich sind. Zudem kann dem Urteil entnommen werden, dass aufgrund der Schwere des vorliegenden Eingriffs das Interesse des Betroffenen gegenüber dem wirtschaftlichen Interesse der Suchmaschinenbetreiber und dem Informationsinteresse der Öffentlichkeit im Grundsatz wohl überwiegen dürfte. In diesem Sinne erscheint das vorliegende Urteil wegweisend für eine allfällig zukünftige Regelung des damit verbundenen «Recht[s] auf Vergessen». Nachfolgend konzentrierte sich der Referent auf weitere, spezifische Fragestellungen, wie beispielsweise die Speicherung von Fingerabdrücken in biometrischen Pässen oder die sog. Vorratsdatenspeicherung, die in der europäischen Rechtsprechung eingehend diskutiert wurden. Mit dem Ausblick auf einige anstehende Entscheidungen wurden zum Schluss zukünftig zu erwartende Entwicklungen skizziert. Ausserdem wurde vor dem Hintergrund der bereits in die Jahre gekommenen datenschutzrechtlichen Grundlagen die erhebliche Bedeutung des *case law* betont. Aufgrund der allfälligen Kodifikation der EuGH-Rechtsprechung in der neuen Datenschutzgrundverordnung und der voraussichtlichen Kontinuität der Rechtsentwicklungen werde deren Relevanz laut dem Referenten wohl auch unter neuem Recht bestehen bleiben.

3. Atelier III: Auswirkungen, Risiken und Chancen der Sammlung physiologischer Daten im Gesundheitsbereich

[Rz 11] In seinem Atelier beschäftigte sich Stéphane Koch, Experte im Bereich neuer Informationstechnologien, mit den Methoden digitaler Selbstvermessung und deren Auswirkungen auf die Privatsphäre des Einzelnen. Im Rahmen des sog. *Quantified Self* werden selbst erfasste, (meist) gesundheitsbezogene Daten analysiert und in statistischer Form ausgewertet, damit der Nutzer seine Aktivitäten und Bewegungen und damit auch seinen körperlichen Zustand laufend überprüfen und reflektieren kann. Als Verwendungszwecke kommen dabei nicht nur medizinische Anwendungen durch den Arzt oder Patienten, sondern auch die Messung sportlicher Leistung und die Stärkung des Wohlbefindens in Betracht. Um den Stellenwert der digitalen Selbstvermessung in der Gesellschaft zu verdeutlichen, zeigte der Referent anhand verschiedener Statistiken auf, welchen Nutzen die AnwenderInnen diesen Instrumenten zusprachen und ob infolge der Selbstvermessung tatsächlich Konsumgewohnheiten geändert wurden. Nachfolgend kam der Referent nicht nur auf die Qualität der erfassten Daten zu sprechen, sondern er erläuterte ebenfalls die allfälligen Nutzungsmöglichkeiten der Datensammlungen durch die Mobiltelefonhersteller, App-Entwickler sowie Versicherungen. Möglich wäre beispielsweise, dass Versicherungen denjenigen Personen eine Prämienreduktion gewähren, die bestimmte Instrumente der digitalen Selbstvermessung verwenden und die daraus gewonnenen Daten der Versicherung zugänglich machen. Obschon der Referent in diesem Zusammenhang von einer *Win-win*-Situation sprach, müsste freilich vorerst abgeklärt werden, ob sich eine solche Abrede mit den datenschutzrechtlichen Vorgaben überhaupt vereinen liesse. Damit kann jedenfalls die These aufgestellt werden, dass sich die Datenschutzexperten zukünftig wohl noch vermehrt mit der Zulässigkeit dieser und sonstiger Verwendungen der aus *Quantified Self* gewonnenen Daten beschäftigen werden.

4. Atelier IV: Persönlichkeitsrechte versus Aufbewahrung und Archivierung von Daten: eine Auslegeordnung

[Rz 12] Mit ihrem Atelier bewegte sich Dr. iur. Sandra Husi-Stämpfli, Stellvertretende Datenschutzbeauftragte des Kantons Basel-Stadt, im Spannungsfeld zwischen Persönlichkeitsschutz und Archivierung. In seiner ursprünglichen Fassung geht der Schutz der Persönlichkeitsrechte auf das verfassungsrechtlich verankerte Recht auf persönliche Freiheit zurück und umfasst daher auch Güter wie die körperliche und geistige Integrität und die Bewegungsfreiheit, wobei in Zusammenhang mit der Archivierung die Achtung der Privatsphäre und der Schutz des gesellschaftlichen Ansehens in besonderem Masse betroffen sind. Im Gegensatz dazu dient die Archivierung öffentlichen Anliegen wie etwa der Dokumentation staatlicher Tätigkeit, der Beweissicherung, der historischen Aufarbeitung sowie der Forschung. Vor diesem Hintergrund ergibt sich im Bereich der Archivierung ein enormes Konfliktpotenzial, das sich gemäss der Referentin mit Blick auf die mit *Big Data* einhergehenden Entwicklungen zunehmend erhöht. Zur Verdeutlichung dieses Spannungsverhältnisses ging die Referentin schliesslich der Frage nach, ob auch unrechtmässig bearbeitete Personendaten einer Archivierung zugänglich sind. Solche Daten hätten zwar grundsätzlich aufgrund der widerrechtlichen Bearbeitung bereits vor der Archivierung ausgesondert und vernichtet werden sollen, könnten aber späteren Generationen bei der Aufarbeitung staatlichen Fehlverhaltens ausgesprochen nützlich sein. Zielführend sind in solchen Fallkonstellationen laut der Referentin einzelfallbezogene Lösungen, die die Abwägung der einander gegenüber stehenden Interessen miteinschliessen. Hingegen bleibt der Umstand bestehen, dass bei der Verhältnismässigkeitsprüfung äusserst schwierig zu beurteilen ist, welche konkreten Dokumente zum Zeitpunkt einer späteren Aufarbeitung oder Beweisführung tatsächlich noch erforderlich sein könnten. Dass die Einhaltung der weiteren Datenschutzgrundätze im Archivwesen ebenfalls mit Schwierigkeiten verbunden ist, zeigte sich in den Diskussionen rund um die Problematik der Verdingkinder. Nachfolgend machte die Referentin zudem darauf aufmerksam, dass sich die Auswirkungen des im *Google*[8]-Urteil vorgebrachten «Recht[s] auf Vergessen» bis auf Weiteres nicht abschätzen liessen. Insbesondere stelle sich dabei die Frage, ob sich die Löschungspflicht in Bezug auf online zur Verfügung gestellte Inhalte auf Archivbestände übertragen lasse und infolgedessen auch bereits archivierte Dokumente regelmässig aussortiert und gegebenenfalls gar gelöscht werden müssten. Für all diese aufgezeigten Problemstellungen seien Lösungswege anzustreben, die – so der Schlussgedanke der Referentin – sowohl die Persönlichkeitsrechte des Betroffenen als auch die öffentlichen Interessen der Archive gebührend berücksichtigen.

IV. Abschliessende Bemerkungen

[Rz 13] *Big Data* eröffnet zwar neue Forschungsperspektiven und birgt grosses ökonomisches Potenzial, stellt aber gleichzeitig das bestehende Datenschutzrecht vor beachtliche Hürden. Denn in diesem Zusammenhang kommen Verarbeitungsmethoden zum Einsatz, die sich mit den herkömmlichen datenschutzrechtlichen Prinzipien, insbesondere dem Zweckbindungsprinzip, dem Verhältnismässigkeitsprinzip und dem Grundsatz der Transparenz kaum vereinen lassen. Dazu kommt, dass aufgrund des mit *Big Data* einhergehenden Risikos der De-Anonymisierung die Frage nach

8 Siehe Fn. 7.

der Anwendbarkeit des Datenschutzrechts erhebliche Schwierigkeiten bereitet. Ferner muss auch das bestehende Einwilligungskonzept als Rechtfertigungsgrund für eine Persönlichkeitsverletzung überdacht werden, scheint doch eine hinreichend aufgeklärte Einwilligung wegen der kaum absehbaren zukünftigen Bearbeitungen kaum jemals vorzuliegen. Zur Lösung dieser Problemstellungen sind nicht nur die im Hinblick auf das geltende Recht bestehenden Möglichkeiten in Betracht zu ziehen. Vielmehr geben diese Herausforderungen gleichzeitig dazu Anlass, die Grundkonzeption des Datenschutzrechts in Frage zu stellen und neue Lösungsansätze ins Auge zu fassen, sei dies in Form von punktuellen Neuerungen oder auch als umfassende Neukonzeption des Datenschutzrechts. Mit letzteren Handlungsmöglichkeiten könnten dabei weitere im Zusammenhang mit dem aktuellen Datenschutzrecht bestehende Problempunkte (z.B. würde die Bildung von Nutzungsgemeinschaften zur gemeinsamen Teilhabe am Wert der Daten auch das Bewusstsein für den Schutz der eigenen Daten stärken) angegangen werden. Jedoch sind solche Massnahmen aufgrund der damit einhergehenden rechtlichen Neuorientierung mit weitgehenden Umsetzungsschwierigkeiten und -unsicherheiten behaftet. Hingegen könnten die Auswirkungen der gestützt auf bestehendem Recht vorgenommenen Anpassungen wohl besser abgeschätzt werden. Nicht nur deswegen dürfte sich auch deren Implementierung um einiges einfacher gestalten. Ungeachtet dessen ist aber letztlich von besonderer Relevanz, dass die getroffenen Massnahmen jedenfalls eine für jeden Einzelfall adäquate und gerechte Lösung vorsehen und damit dem Schutz der Persönlichkeitsrechte des Einzelnen bestmöglich Rechnung tragen.

Daniela Nüesch, MLaw ist als diplomierte Assistentin am Institut für Europarecht an der Universität Freiburg i.Ue. tätig.
Für die wertvollen Anregungen bei der Erarbeitung des vorliegenden Beitrags und die kritische Durchsicht des Manuskripts geht mein herzlicher Dank an Frau Prof. Astrid Epiney, Herrn Dr. Markus Kern und Herrn Tobias Auer.