Begrüßung

Dr. Armin Bammer, Rechtsanwalt in Wien,
Vizepräsident der Österreichischen Juristenkommission

Sehr geehrte Damen und Herren, herzlichen Dank, dass so viele von Ihnen aus ganz Österreich hierher in die Donauschlinge gekommen sind. Mein Name ist *Armin Bammer*, ich vertrete als Vizepräsident unseren leider erkrankten Präsidenten *Rudolf Müller*, der sich erholt und sich diesen doch nicht geringen Strapazen besser nicht aussetzt. Seine Funktionen werde ich mir mit *Eva Schulev-Steindl*, der 2. Vizepräsidentin, und *Eva Souhrada-Kirchmayer* aufteilen.

Unsere Tagung befasst sich mit dem Datenschutz, ein Thema, mit dem wir uns als Juristenkommission schon einmal im Jahre 2009 unter dem Titel „Alles unter Kontrolle? Überwachung – Privatsphäre – Datenschutz" befasst haben. Diese seinerzeitige Tagung entstand unter anderem deshalb, weil die Deutsche Sektion der Internationalen Juristenkommission im Jahr 2007 in Leipzig eine Datenschutztagung gemacht hat. Sie sehen also, Datenschutz ist ein Thema, das die Juristenkommissionen im internationalen Kontext sehr interessiert, nicht zuletzt deshalb, weil es einen sehr starken grundrechtlichen Bezug gibt. Grundrechte waren in Europa seit 1945 noch selten so gefährdet wie heutzutage. Das hat zumindest drei Ursachen: Die reale und latente Terrordrohung, die über den europäischen Staaten liegt, die Flüchtlingskrise mit Migrationsdruck und als dritten Grund die neuen politischen Strömungen, die sich dieser beiden Krisen zwar bedienen, denen aber auch noch aus anderen Gründen die Grundrechte bei der Verfolgung ihrer autoritären Ziele im Wege stehen. Vielleicht nicht nur die Grundrechte, sondern überhaupt eine unabhängige Justiz und eine unabhängige Verfassungsgerichtsbarkeit.

Die Österreichische Juristenkommission leidet daher nicht gerade an einem Themenmangel, vor allem unter dem Gesichtspunkt unserer selbst auferlegten „Watchdog-Funktion". Grund- und Freiheitsrechte – und da insbesondere das Grundrecht auf Datenschutz – sind in mehrfacher Hinsicht herausgefordert. Wir werden versuchen, nicht nur die grundsätzlichen, die grundrechtlichen und die allgemeinen Bezüge des Themas „Datenschutz" darzustellen, die über DSGVO-Detailprobleme hinausgehen, sondern vielleicht auch zB die Frage des Datenschutzes beim Reisen – „Passenger Name Records" und andere Dinge mehr, die jetzt nicht spezifisch DSGVO-Fragen betreffen.

Aktuelle Bedrohungen des Grundrechts auf Privatsphäre

Walter Berka

I. Das neue Paradigma der „Post-Privacy"

Nachdem im Frühjahr 2018 der Datenskandal rund um *Facebook* und *Cambridge Analytica* die Öffentlichkeit empört hatte und *Mark Zuckerberg* gezwungen worden war, den Missbrauch der Daten von mehr als 80 Millionen Menschen mehr oder minder reuig einzugestehen, forderten Politiker lautstark eine stärkere Regulierung von *Facebook* und prominente User sowie große Unternehmen kündigten demonstrativ ihren Rückzug von *Facebook* an. Was ist tatsächlich geschehen? Wenige Wochen nach dem Ausbruch der allgemeinen Empörung war die Nutzerzahl der Plattform um weitere 13 % auf 2,2 Milliarden Menschen angestiegen und haben sich die Gewinne des Unternehmens aus dem Werbegeschäft angeblich um rund 60 % erhöht. Auch in Österreich wollte nach einer aktuellen Umfrage nur ein Bruchteil der Menschen seinen Facebook-Account löschen.

Wollen die Menschen überhaupt noch einen Schutz ihrer Privatsphäre, brauchen sie ihn noch? „*Privacy is doomed … get used to it*", titelte der *Economist* schon gegen Ende des 20. Jahrhunderts[1] und so ist es nicht erstaunlich, wenn der Gründer von *Facebook* von einem „*Post-Privacy*"-Zeitalter sprach, das er selbst für erwünscht und unentbehrlich hält.[2] Tatsächlich gehört die Erosion der Privatsphäre zu den großen gesellschaftspolitischen Themen des letzten Jahrzehnts und alles, was dazu geschrieben wird, diagnostiziert den Verfall: *The Destruction of Privacy, The Death of Privacy, The End of Privacy, Privacy Under Attack, Privacy: The Lost Right, Goodbye Privacy* sind nur einige einschlägige Titel einer Aufzählung von aktuellen Veröffentlichungen, die sich unschwer fortsetzen ließe.[3] Klagen über den Verlust der Privatsphäre hat es freilich schon immer gegeben und das, was wir die Privatsphäre nennen, ist tatsächlich nichts real Vorgegebenes, sondern ein soziales Konstrukt.[4] Daher ist die Vorstellung von einer schutzwürdigen oder verfassungsrechtlich geschützten Privatheit wandelbar, und das Gleiche muss auch für die Bedrohungen gelten, die als aktuelle Bedrohungen wahrgenommen werden.

Damit bin ich bei dem hier gestellten Thema. Was sind die aktuellen Bedrohungen des Grundrechts auf Privatsphäre? An sich sind sie bekannt und so glaube ich nicht, dass ich viel Neues erzähle: Wer ein Smartphone in der Tasche trägt, weiß

1 Zu diesem Zitat und seiner Geschichte vgl *Bennett/Raab*, The Governance of Privacy (2006) 7 f.

2 Vgl den Nachweis bei http://www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html (abgerufen 7.5.2018). Zur sogenannten „Post-Privacy-Debatte" vgl ferner *Boehme-Neßler*, Big Data und Demokratie – Warum Demokratie ohne Datenschutz nicht funktioniert, DVBl 2015, 1282 (1284); *Bosesky/Brüning*, Verständnis und Schutz von digitaler Privatheit im nationalen Recht, in *Hill/Schliesky* (Hrsg), Die Neubestimmung der Privatheit (2014) 79 (86 ff).

3 Vgl die Nachweise zu diesen Titeln bei *Berka*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, Verhandlungen des 18. ÖJT I/1 (2012) 9.

4 *Nettesheim*, Grundrechtsschutz der Privatheit, VVDStRL 70 (2011) 7 (9 ff); *Albers*, Grundrechtsschutz der Privatheit, DVBl 2010, 1061 (1063) jeweils mwN. Zum Paradigma der Privacy aus einer sozialwissenschaftlichen Perspektive *Bennet/Raab* (Fn 1) 4 ff.

oder sollte zumindest wissen, dass er eine kontinuierliche Datenspur hinterlässt, die erfasst, wohin er sich begibt, wo er einkauft und mit welchen Kontakten er kommuniziert. Das ist eine Folge der Miniaturisierung der digitalen Endgeräte und ihrer Vernetzung. Wenn die so erfassten Daten irgendwo in einer digitalen Cloud gespeichert werden, werden die Folgen der Globalisierung der Datenströme sichtbar, welche die Zuordnung von greifbaren Verantwortlichkeiten und den Zugriff nationalstaatlicher Regelungsautorität erschwert. Zusammengenommen hat beides die Zugriffsmöglichkeiten mächtiger globaler Unternehmen enorm erweitert und faktisch jede wirksame Kontrolle der Datenströme unmöglich gemacht. Man könnte über das Internet der Dinge sprechen, das dazu führt, dass vielfältige Lebensäußerungen der Menschen digital erfasst, vernetzt und somit kontrollierbar werden. Dass die Menschen selbst dazu beitragen, weil sie freiwillig jede noch so private Gegebenheit bis hin zur Pulsfrequenz, den Kalorienverbrauch und das Körpergewicht in den sozialen Netzwerken teilen und bereitwillig hinausposaunen, was sie essen, wen sie lieben und was sie sonst noch so treiben, trägt dazu bei. Die Entblößung des Privaten findet in großem Umfang freiwillig statt und anscheinend kann man mit *Facebook-Likes* menschliches Verhalten besser vorhersagen, als das die besten Freunde oder die Familie könnte.[5] Man müsste auf den ungezügelt fortschreitenden Ausbau der staatlichen Überwachung hinweisen, die den Behörden mit immer neuen und invasiven Instrumenten den Zugriff auf das Geschehen in den öffentlichen Räumen, auf die Bewegungsprofile der Menschen und auf ihre private Kommunikation ermöglicht. Und nicht erst seit den Enthüllungen durch *Edward Snowden* wissen wir, in welchem Ausmaß Daten durch die Geheimdienste abgesaugt werden, und zwar ohne Rücksicht auf die Rechtmäßigkeit oder Rechtswidrigkeit der weltumspannenden, geheim gehaltenen Überwachung der Telekommunikation und des Internet. Man könnte auf den Umstand zu sprechen kommen, dass mit den Möglichkeiten des *Data Mining* und der Auswertung von *Big Data* private Sachverhalte kollektiviert werden, zum Nutzen der Menschen, etwa im Rahmen der präventiven Gesundheitsvorsorge oder einer zielgerichteten Steuerung von Erziehungs- und Bildungsprozessen, aber auch zu ihrem Nachteil, wenn immer enger geknüpfte Profile angelegt werden können.[6] Die Macht der Algorithmen macht uns zu Gefangenen von Wahrscheinlichkeiten, die niemand mehr durchschauen kann, die aber unser Leben zunehmend mehr bestimmen, wenn wir etwa eine Versicherung abschließen, eine Arbeitsstelle suchen oder Waren einkaufen.[7] Dass eine umfassende Verhaltenssteuerung schon eine mögliche nahe Zukunft ist, zeigen die in China laufenden Versuche mit einem Sozialkreditsystem, also einem gesell-

5 Vgl dazu unter Bezugnahme auf *Han*, Psychopolitik (2014) 18 f, 54 f und mit weiteren Nachweisen *Pöschl*, Sicherung grund- und menschenrechtlicher Standards gegenüber neuen Gefährdungen durch private und ausländische Akteure, VVDStRL 74 (2015) 405 (421).

6 Vgl die Beiträge in *Hoffmann-Riem* (Hrsg), Big Data. Regulative Herausforderungen (2018) passim.

7 Vgl *Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen. Eine Herausforderung für das Recht, AöR 142 (2017) 1 (6 ff).

schaftlichen Steuerungssystem, bei welchem der Zugang zu sozialen Leistungen oder auch nur zu Verkehrsmitteln von einem digitalen *Scoring*, also von angesammelten Punkten der Vertrauenswürdigkeit und des sozialen Wohlverhaltens, abhängt.[8]

Das alles ist bekannt, darüber wird im Rahmen des rechtspolitischen Diskurses und gesellschaftspolitischer Kontroversen diskutiert und damit müssen sich gelegentlich die Gerichte auseinandersetzen, wenn sie im Einzelfall die Grenzen bestimmen, die dem Zugriff auf private Daten gesetzt sind, und wenn sie die Rechtsbehelfe klären, die vor ihrem Missbrauch schützen. Was ist aber das eigentliche Schutzgut, um das sich alles dreht? Was ist der wahre Grund unserer Besorgnis? Ist es noch die Privatsphäre oder die Privatheit, von der – wenn ich nochmals an die Eingangszitate erinnere – viele sagen, dass sie zu einem Ende gekommen ist? Sind wir tatsächlich schon im Zeitalter einer „*Post-Privacy*" angelangt? Wenn man so fragt, sollte man nicht bei einzelnen Bedrohungsszenarien stehen bleiben, sondern sollte das Thema ins Grundsätzliche wenden: Welches Rechtsgut ist es oder welche Rechtsgüter sind es, die bedroht werden, wenn sich der Staat oder mächtige Private persönlicher Daten in einem Maße wie niemals zuvor bemächtigen? Dazu sollen im Folgenden einige Überlegungen angestellt werden, verbunden mit der Hoffnung, dass eine Antwort auf diese Frage auch zeigen könnte, was die wirklich aktuellen Herausforderungen sind, wenn wir vom Schutz der Privatheit unter den Bedingungen des digitalen Informationszeitalters sprechen.

II. Regulative Konzeptionen des Datenschutzrechts

A. Die Tradition des Privacy-Schutzes

Der Schutz der Menschen vor einem Missbrauch der sie betreffenden Informationen hat sich zeitlich in mehreren Entwicklungsstufen und in verschiedenen Rechtstraditionen entfaltet.

Als sich zum ersten Mal in den 1960er-Jahren die Möglichkeiten und Risiken der automatisierten Datenverarbeitung abzuzeichnen begannen, war es das Konzept einer rechtlich geschützten Privatsphäre, auf das sich die einsetzende datenschutzrechtliche Rechtsetzung bezog. Datenschutz war Privatheitsschutz, Schutzgut war die Privatsphäre und nicht Daten *per se*. Paradigmatisch für diesen Ansatz war das US-amerikanische Recht, das auf die schon älteren

8 Einen guten Überblick über diese und andere Herausforderungen bieten die Berichte des Sonderberichterstatters des UN-Menschenrechtsrats für das Recht auf Privatsphäre mit der Auflistung von Problemfeldern; vgl zB Human Rights Council, Report of the Special Rapporteur on the right to privacy, *Joseph A. Cannataci*, A/HRC/31/64, 8.3.2016 sowie die nachfolgenden Berichte (abrufbar unter https://www.privacyandpersonality.org/un-reports/human-rights-council-reports/[abgerufen 7.5.2018]).

Rechtstraditionen des *Privacy*-Schutzes aufbauen konnte.[9] Der hier gebotene Schutz kommt den privaten Daten der Menschen zu, entsprechend einem „*Right to be let alone*", und er richtet sich in erster Linie gegen Übergriffe des Staates. Der freie gesellschaftliche Informationsverkehr einschließlich der kommerziellen Verwertung von Daten wird nur sehr begrenzt und in besonders sensiblen Bereichen Beschränkungen unterworfen, etwa im Zusammenhang mit dem Kredit- und Versicherungswesen.[10] Auf einen engeren Bereich der Privatsphäre bezogen sind datenschutzrechtliche Schranken die Ausnahme und wird eine umfassende Reglementierung des Datenverkehrs gar nicht angestrebt. Maßnahmen der Selbstregulierung haben Vorrang gegenüber behördlicher Intervention. *Privacy* ist so gesehen ein limitiertes Recht unter anderen.

Ein solches Modell eines begrenzten und primär auf die Privatsphäre bezogenen Datenschutzrechts ist (etwas vereinfacht gesagt) für das US-amerikanische Recht bis heute prägend. Das ist auch, wie am Rande anzumerken ist, der Grund für die tief greifenden Konflikte, die es im Zusammenhang mit dem transatlantischen Datenverkehr schon seit Jahrzehnten gibt und das entsprechende Misstrauen zwischen den USA und Europa.[11]

Ein solcher Schutz der Privatsphäre ist bis heute wichtig und nicht überholt: Die berechtigte Sorge vor jedem weiteren Ausbau staatlicher Zugriffsmöglichkeiten, etwa in der Form der nunmehr auch in Österreich für zulässig erklärten Verwendung von Spionagesoftware, mit welcher der Staat in private Computer oder Smartphones einzudringen vermag, zeigt das deutlich. Andererseits lässt sich nicht übersehen, dass die sozialen Räume des Privaten und des Öffentlichen in der Gegenwart zunehmend verschwimmen. Die Grenzen zwischen dem, was die Allgemeinheit angeht, und dem, was der privaten Beliebigkeit überlassen bleibt, haben sich aufgelöst (wobei nochmals anzumerken ist, dass diese Grenzen immer schon kontingent waren). Das Internet und hier wiederum die sozialen Medien sind geradezu paradigmatisch zu einem Raum geworden, in dem die Gleichzei-

9 Zur Entwicklung des Privatheitsschutzes in den USA vgl zB *Brugger*, Der grundrechtliche Schutz der Privatsphäre in den Vereinigten Staaten von Amerika, AöR 108 (1983) 25; zum Datenschutzrecht *Regan*, The United States, in *Rule/Greenleaf* (Hrsg), Global Privacy Protection. The First Generation (2010) 50.

10 Das mag mit grundlegenden Unterschieden im amerikanischen und europäischen Freiheits- und Grundrechtsverständnis zusammenhängen; vgl mit unterschiedlichen Akzenten *Whitman*, The Two Western Cultures of Privacy: Dignity versus Liberty, Yale Law Journal 113 (2004) 1151 (insbesondere 1190 ff); *Diggelmann*, Grundrechtsschutz der Privatheit, VVDStRL 70 (2011) 50 (69 ff).

11 Vgl dazu jeweils mwN *Klar/Kühling*, Privatheit und Datenschutz in der EU und den USA – Kollision zweier Welten? AöR 141 (2016) 165; *Bygrave*, International agreements to protect personal data, in *Rule/Greenleaf* (Hrsg), Global Privacy Protection. The First Generation (2010) 15 ff; zu den handelspolitischen Komplikationen im transatlantischen Datenverkehr *Berka*, CETA, TTIP, TiSA, and Data Protection, in *Griller/Obwexer/Vranes* (Hrsg), Mega-Regional Trade Agreements: CETA, TTIP, and TiSA (2017) 175. Zur Frage, ob dem europäischen Datenschutzkonzept tatsächlich eine nachhaltige Vorbildwirkung zukommen wird können, vgl insoweit vorsichtig optimistisch *Wagner*, Wie weit reicht der universelle datenschutzrechtliche Konsens? ZÖR 73 (2018) 113.

tigkeit der Sphären des Privaten und Öffentlichen zum Tragen kommt, wobei es häufig unklar und unvorhersehbar ist, ob und wann genau eine Botschaft oder Unterhaltung von der einen in die andere Sphäre übergeht. Das Privateste kann und wird öffentlich gemacht, während genuin öffentliche Angelegenheiten der Politik oder Gesellschaft im Modus privater Zufälligkeit behandelt werden. Und bei der Verarbeitung von *Big Data* mit den heutigen und künftigen Mitteln der Datenanalyse wird zwangsläufig auf private Daten zugegriffen, dies freilich mit dem Ziel, gesellschaftliche und kollektive Entwicklungen zu prognostizieren oder zu steuern. Ein auf den Schutz der Privatheit fokussierter Datenschutz greift in solchen Zusammenhängen zu kurz.[12]

B. Das Grundrecht auf informationelle Selbstbestimmung

Die europäische Tradition des Datenschutzrechts baut ebenfalls auf den Schutz der Privatheit auf, wobei dieser Anspruch allerdings von Anfang an nicht als ein Recht unter anderen, sondern als ein fundamentales Persönlichkeitsrecht aufgefasst wurde. Die Grenzen eines Privatheitsschutzes wurden in Europa allerdings bald überschritten. Als die ersten europäischen Datenschutzgesetze verabschiedet wurden, hatte man die damals neuen Möglichkeiten der automatisierten Datenverarbeitung zur Speicherung und Verarbeitung großer Datenmengen vor Augen. Daher wurde im Prinzip überzeugend argumentiert, dass es keine Informationen mehr geben könne, die für sich genommen mehr oder weniger schutzbedürftig sind. Denn schutzwürdige Interessen des Einzelnen können auch dann massiv beeinträchtigt werden, wenn vielfältige, an sich „harmlose" Daten rasch und massenhaft zusammengeführt und verknüpft werden. In der Konsequenz musste das bedeuten, dass letztlich alle Daten, die einen Schluss auf eine bestimmte Person zulassen, ohne Rücksicht auf den Inhalt schutzbedürftig geworden waren. Wenn jede personenbezogene Information die „*Vermutung eines privaten Charakters*" in sich trägt,[13] verliert das Paradigma der Privatsphäre seine Tragfähigkeit. Schutzobjekte sind dann nicht mehr nur Informationen aus einem Privatbereich, sondern alle personenbezogenen Daten.[14] Vom Schutzzweck her betrachtet zielt dieser Ansatz über den Privatheitsschutz hinausgehend auf ein „Recht auf informationelle Selbstbestimmung", also auf den Anspruch, als „Herr über seine Daten" prinzipiell selbst entscheiden zu dürfen, mit wem und zu wel-

12 Dazu, dass der Privatheitsschutz jedenfalls eine gewisse, wenngleich relative, Trennung von Öffentlich und Privat voraussetzt, vgl zB *Bennett/Raab* (Fn 1) 4 ff mwN.

13 So zB *Seidel*, Datenbanken und Persönlichkeitsrecht (1972) 67. Zur terminologischen Abkoppelung des Begriffs „Datenschutz" vom „Privacy"-Konzept bezogen auf die Entwicklung des österreichischen Rechts vgl *Duschanek*, Die Entwicklung des Datenschutzes in Österreich, in *Bauer/Reimer* (Hrsg), Handbuch Datenschutzrecht (2009) 43.

14 Vgl zu den unterschiedlichen Konzepten der geschützten Daten im Rechtsvergleich *Schwartz/Solove*, Reconciling Personal Information in the United States and European Union, California Law Review 102 (2014) 877 (878 ff).

chem Zweck ich die mich betreffenden Informationen mit anderen teile. Dieses Recht auf informationelle Selbstbestimmung wurde zur „Magna Charta" des Datenschutzes, das im Rahmen eines bürokratisch konzipierten Datenschutzrechts detailreich und mit einem übergreifenden Geltungsanspruch kodifiziert wurde. Mit der Verankerung eines eigenständigen Datenschutzgrundrechts im österreichischen DSG und sodann in der Europäischen Grundrechtecharta wurde der Anspruch auf informationelle Selbstbestimmung auch grundrechtlich verbürgt.[15] Es ist dieser Ansatz, der bis heute den kontinentalen Datenschutz charakterisiert, bis hin zur DSGVO, die sich ebenfalls noch diesem traditionellen Konzept verpflichtet weiß.[16]

Ein Recht auf informationelle Selbstbestimmung beruht auf dem Prinzip der individuellen Kontrolle über personenbezogene Daten und auf der Annahme, dass der Umgang mit solchen Daten die rechtfertigungsbedürftige Ausnahme ist und bleiben soll. Ob diese Prämissen beim Wort genommen jemals richtig waren, ist fraglich.[17] Unter den heutigen Bedingungen sind sie jedenfalls nur mehr begrenzt tragfähig. Daten sind – wie gesagt wurde – nicht das Gift, sondern das Blut der Informationsgesellschaft,[18] und das gilt auch für den Datenverkehr als nicht hinwegzudenkende Ressource einer Informationsgesellschaft. Das drückt sich auch im sogenannten *Privacy*-Paradoxon aus: Zwar erklären die meisten Menschen, dass ihnen der Datenschutz ein wichtiges Anliegen ist, aber die wenigsten sind bereit, irgendwelche Anstrengungen zu unternehmen, um ihre persönlichen Daten tatsächlich zu schützen. Wer nicht als digitaler Eremit leben möchte, muss unter den heutigen Bedingungen bereit sein, seine Zustimmung zur alltäglichen und vielfältigen Nutzung seiner Daten zu geben, und er tut das auch. Die Menschen geben ihre Zustimmung, auch wenn sie wissen oder wissen müssten, dass ihre Daten in einer Weise verwendet werden, die sie nicht mehr kontrollieren können. Ständiger Datenaustausch ist nicht die Ausnahme, sondern ist zur Normalität geworden.

15 Vgl zur grundrechtlichen Gewährleistung eines solchen Rechts *Grabenwarter*, Das Recht auf informationelle Selbstbestimmung im Europarecht und im Verfassungsrecht, AnwBl 2015, 404; auch der VfGH und der EGMR leiten aus Art 8 EMRK ein Recht auf informationelle Selbstbestimmung bzw ein „right to informational self-determination" ab; vgl VfSlg 19.892/2014 sowie EGMR 27.6.2017, Nr 931/13 – Satakunnan Markkinapörssi Oy and Satamedia Oy, § 137.

16 Zu unterschiedlichen theoretischen Konzeptionen des Datenschutzrechts und des Verhältnisses zwischen Privacy und Datenschutz vgl mwN *Tzanou*, The Fundamental Right to Data Protection (2017) 24 ff.

17 Vgl zur begrenzten Überzeugungskraft eines solchen Rechts auf informationelle Selbstbestimmung *Ladeur*, Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion? DÖV 2009, 45; *Hoffmann-Riem*, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998) 513 (519 ff); *Albers* (Fn 4) DVBl 2010, 1068.

18 *Hoffmann-Riem*, Verwaltungsrecht in der Informationsgesellschaft – Einleitende Problemskizze, in *Hoffmann-Riem/Schmidt-Aßmann* (Hrsg), Verwaltungsrecht in der Informationsgesellschaft (2000) 9 (55).

Was ist das Fazit? Ein Schutz der Privatsphäre und der privaten Daten ist wichtig und auch unter den heutigen Bedingungen unverzichtbar. Das Gleiche gilt für den Grundsatz der informationellen Selbstbestimmung, also für das Prinzip der individuellen Kontrolle über die mich betreffenden Daten. Aber es ist fraglich, ob wir mit diesen Ansätzen bereits die Mittel und Maßstäbe in der Hand haben, um den Umgang mit Informationen, die uns betreffen, und den möglichen Missbrauch dieser Daten angemessen zu erfassen. Denn worum geht es heute wirklich?

III. Die gefährdete Autonomie des Einzelnen

A. Targeted Advertising als Beispiel

Man kann von einer alltäglichen Erfahrung ausgehen: Jeder von uns, der gelegentlich oder auch häufiger Waren oder Dienstleistungen im Internet erwirbt, hat Erfahrungen mit zielgerichteter Werbung (*Targeted Advertising*) gemacht. Werbung wird individuell platziert, und das ist möglich, weil früheres Kaufverhalten, die Websites, die jemand ansteuert, erkennbare persönliche Vorlieben und andere persönliche Daten erfasst, ausgewertet und zu einer zielgruppenspezifischen oder individuellen Adressierung der Konsumenten verwendet werden. Kaufverhalten wird somit durch zielgerichtete Werbung gesteuert, und zwar sehr viel effektiver und unter Vermeidung der Streuverluste, die es bei jeder anderen Werbeform gibt. Dies kann man im Einzelfall als Vorteil wahrnehmen, der es auch tatsächlich sein kann. Man mag mit Interesse registrieren, was das Netz schon alles über seine Nutzer weiß. Oder man sieht es als Ärgernis und Beweis für den alltäglichen Datenmissbrauch an: Wie immer wir solche Werbepraktiken bewerten, sie zielen auf eine verhaltenssteuernde Wirkung. Sie beeinflussen unser Verhalten als Konsumenten und sie betreffen Entscheidungen, die wir dem Paradigma des aufgeklärten, mündigen Konsumenten entsprechend grundsätzlich selbst als autonome, selbstbestimmte Subjekte treffen sollten.

Nun ist die manipulative Kraft der kommerziellen Werbung nichts wirklich Neues und sind unsere alltäglichen Entscheidungen als Konsumenten wahrscheinlich niemals ganz autonom und unbeeinflusst gewesen. So gesehen sollte man das Gefahrenpotenzial von *Targeted Advertising* nicht dramatisieren. Möglichen Missbräuchen wird man mit den Mitteln des Wettbewerbsrechts begegnen können.

B. Verhaltenssteuerung durch Informationsmacht

Verhaltenssteuerung durch Informationsmacht ist allerdings nicht nur ein Problem des Konsumentenschutzes. Mit den heutigen Möglichkeiten der Datenauswertung unter den Vorzeichen von *Big Data* und *Data Mining* kann jeder soziale

Lebensbereich und können alle Lebensäußerungen auf der Grundlage massenhaft verfügbarer Daten nach Wahrscheinlichkeiten und Korrelationen durchsucht und zum Gegenstand sozialer Kontrolle und Steuerung gemacht werden. Seit Kurzem wissen wir, dass demokratische Wahlen durch zielgerichtete Werbung, durch die Platzierung von *Fake News* und durch automatisierte Bots gesteuert und manipuliert werden. Das ist es, was den bekannt gewordenen Datenmissbrauch durch *Facebook* tatsächlich zum beunruhigenden Skandal macht. Plötzlich geht es nicht mehr um die Entscheidung zwischen mehr oder minder belanglosen Konsumgütern, sondern um die Grundlagen des demokratischen Verfassungsstaates: Es geht um die Korrektheit der demokratischen Wahlen, die Unbeeinflusstheit des Wählerwillens und die notwendige Annahme, dass Wahlen Ausdruck möglichst rationaler und persönlich verantworteter Entscheidungen mündiger Bürgerinnen und Bürger sind. Und was für Wahlen gilt, muss auch für Abstimmungen und andere Entscheidungen in Angelegenheiten der *Res Publica* gelten, sodass es ebenso ein Skandalon ist, wenn sich die Vermutungen bestätigen, dass die englische Mehrheit für den *Brexit* durch bewusst platzierte Fehlinformationen und andere Manipulationen zustande gekommen ist. Alles das trifft das Herz der Demokratie.[19]

Auch losgelöst von Wahlen oder Abstimmungen ist die Manipulation der öffentlichen Meinungsbildung durch den massiven Einsatz automatisierter und durch undurchsichtige Algorithmen gesteuerter Programme besorgniserregend. Wenn Menschen auf den heutigen Foren der Meinungsbildung, und das sind die sozialen Medien, nur mehr das lesen oder diskutieren, was ihnen gezielt zugespielt wird, wenn sie ihre „Filterblasen" und „Echokammern" gar nicht mehr verlassen und wenn Wahrheit zur Beliebigkeit wird, verkommt die öffentliche Meinungsbildung. Auch sie ist eine Voraussetzung der demokratischen Gesellschaftsordnung und, darüber hinausgehend, des bewussten Lebens in einer menschlichen Gemeinschaft mit geteilten und gemeinsam diskutierten Werten und Überzeugungen. Eine Gesellschaft zerfällt ohne selbstbewusste Öffentlichkeit.

Datenmissbrauch kann über die erwähnten demokratiepolitischen Zusammenhänge hinausgehend die Entfaltung des Einzelnen in der Gesellschaft gefährden und bisher unbekannten Risiken aussetzen. Auch hier geht es zum einen um den Missbrauch der Möglichkeiten moderner Datenanalyse, die durch die Macht der hinter den Kulissen wirksamen Algorithmen in unser Leben eingreift. *Big Data* kann die Entscheidungsspielräume des Einzelnen verengen und ihn zum Opfer von Wahrscheinlichkeiten machen, die spekulative Rückschlüsse von einem kollektiven Gruppenverhalten auf seine Person zulassen, aber nicht zutreffen müs-

19 Vgl mwN *Kirste*, Automatisierung im Recht, in *Spiel/Neck* (Hrsg), Automatisierung: Wechselwirkungen mit Kunst, Wissenschaft und Gesellschaft (2018) im Druck; zum Brexit-Fall *Deakin*, Information, Responsibility and Democracy: The Case of Brexit, in *Koziol* (Hrsg), Tatsachenmitteilungen und Werturteile: Freiheit und Verantwortung (2018) 147.