Schriften zum Öffentlichen Recht

Band 1301

Das IT-Grundrecht

Schnittfelder und Auswirkungen

Von

Markus Hauser

Duncker & Humblot · Berlin

MARKUS HAUSER

Das IT-Grundrecht

Schriften zum Öffentlichen Recht

Band 1301

Das IT-Grundrecht

Schnittfelder und Auswirkungen

Von

Markus Hauser

Duncker & Humblot · Berlin

Die Fakultät für Rechtswissenschaft
der Universität Hamburg
hat diese Arbeit im Jahr 2014
als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische Daten
sind im Internet über http://dnb.d-nb.de abrufbar.

Fremddatenübernahme: L101 Mediengestaltung, Berlin
Druck: CPI buchbücher.de, Birkach
Printed in Germany

ISSN 0582-0200
ISBN 978-3-428-14643-7 (Print)
ISBN 978-3-428-54643-5 (E-Book)
ISBN 978-3-428-84643-6 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2014 von der rechtswissenschaftlichen Fakultät der Universität Hamburg als Dissertation angenommen. Später erschienene Literatur konnte für die Drucklegung noch bis zum April 2015 berücksichtigt werden.

Mein Dank gilt Frau Prof. Dr. Marion Albers für die fachliche Betreuung der Arbeit über zwei Universitäten hinweg und wertvolle Anregungen. Herrn Prof. Dr. Wolfgang Schulz danke ich für die Anfertigung des Zweitgutachtens.

Persönlich möchte ich meinen Eltern, meinen Freunden und Kollegen für die Unterstützung in der Zeit der Entstehung dieser Arbeit und darüber hinaus danken.

Markus Hauser

Inhaltsverzeichnis

A. Einleitung

I. Ein neuer Ansatz für den Persönlichkeitsschutz

1. Einführung

In nahezu jedem Lebensbereich kommen Bürger und Staat inzwischen mit elektronischer Datenverarbeitung in Berührung. Dabei fallen zwei Entwicklungen auf: Zum einen halten Datenverarbeitungssysteme mehr und mehr Einzug in das private Umfeld des Einzelnen. Wo früher Großrechenanlagen für unternehmerische oder staatliche Zwecke eingesetzt wurden, finden sich nun Personal Computer, Laptops, Smartphones und Tablets in den Haushalten und Jackentaschen der Bürger. Solche Systeme sind dabei nicht mehr nur isolierte Arbeits- oder Unterhaltungsgeräte. Sie werden vielmehr zunehmend mit der Lebensgestaltung selbst verflochten. Durch zahlreiche Erfassungsmöglichkeiten und die fortschreitende Vereinfachung ist eine zunehmende Digitalisierung verschiedenster Persönlichkeitsäußerungen zu beobachten.[1] Damit wachsen zunächst Datenbestände im – vermeintlichen – Einflussbereich des Einzelnen, denen bereits aus ihrer Quantität und Qualität heraus eine hohe Aussagekraft über die Persönlichkeit des Betroffenen zukommt. Parallel zu dieser Entwicklung schreitet auch die elektronische Vernetzung weiter voran. Das Internet hat als ubiquitäres Medium – ähnlich wie die Datenverarbeitungsanlagen – Einzug in die persönliche Lebensgestaltung der Bürger gehalten. Neben der Recherche von Daten zu eigenen Zwecken sind neue Möglichkeiten entstanden, Inhalte mit Dritten oder der Öffentlichkeit zu teilen.

Den Chancen dieser neuen Technologien stehen jedoch vielfältige Risiken für die Belange des Einzelnen gegenüber, die durch die Verzahnung von dezentraler Datenverarbeitung und elektronischer Kommunikation verstärkt werden. Die Begehrlichkeiten Dritter sind vielgestaltig. Sie richten sich zum einen auf die Erforschung der Teilnahme des Einzelnen an Kommunikationsvorgängen. Aber auch die Endgeräte selbst rücken verstärkt in den Fokus, versprechen sie doch tiefere Einblicke in die Persönlichkeit des Nutzers und Zugriff auf sonst kaum zu erlangende Daten. Eine zunehmend dauerhafte Vernetzung durch permanente Internetverbindungen und die Übersim-

---

[1] Vgl. *Schaar*, in: Vieweg/Gerhäuser, Digitale Daten, S. 64: „Automatisierung bereits in der Erhebungsphase“.

plifizierung eigentlich komplexer Zusammenhänge durch immer einfachere Benutzerschnittstellen erhöhen die Risiken von Persönlichkeitsbeeinträchtigungen weiter.

Das vorgefundene Grundrechtsgefüge schützt in vernetzten Zusammenhängen bereits Privatheitserwartungen[2]: Spezielle Gewährleistungen finden sich zunächst in Artt. 10 und 13 GG. Hinzu treten mit dem Recht auf Achtung der Privatsphäre und dem Recht auf informationelle Selbstbestimmung Ausprägungen des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

Personal Computer und ähnliche Geräte wurden dagegen bis vor Kurzem nicht als eigenständige Anknüpfungsobjekte für grundrechtliche Schutzmechanismen erkannt. Gleichwohl bündeln sich in ihnen spezifische Privatheitserwartungen. Sieht man von der grundsätzlichen Möglichkeit des Totalverzichts ab, ist der Einzelne zunehmend auf diese informationstechnischen Systeme in seinem Umfeld und auf deren Zuverlässigkeit angewiesen. Gleichzeitig sind gerade diese Systeme spezifischen Gefahren ausgesetzt.

2. Vertraulichkeit und Integrität informationstechnischer Systeme

Am 27. Februar 2008 hat der erste Senat des Bundesverfassungsgerichts anlässlich der Entscheidung zur sogenannten Online-Durchsuchung das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Fallgruppe des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ausgeformt. Staatliche Ermittler haben aus der Verbreitung von (vernetzten) dezentralen Datenverarbeitungssystemen und damit verbundenen technischen Entwicklungen den Wunsch abgeleitet, wie bereits private Hacker viele Jahre zuvor Zugriff auf diese Systeme zu erlangen.

In seiner Genese unterscheidet sich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gerade dadurch vom Recht auf informationelle Selbstbestimmung, dass eine *spezifische Privatheitserwartung* ausgemacht wird, die eine konkrete thematische Anknüpfung ähnlich dem Wohnungsschutz aus Art. 13 GG ermöglicht. Das Bundesverfassungsgericht hat in seiner Entscheidung mit dem informationstechnischen System (IT-System) einen Topos hervorgehoben, der ohnehin bereits seit längerer Zeit ein wichtiger Faktor im Leben und für das Leben

---

[2] Vgl. *Albers*, DVBl. 2010, 1061 ff. zu den Dichotomien der Privatheit; *Benda*, in: ders./Maihofer/Vogel, Handbuch Verfassungsrecht, 2. Auflage, § 6 Rn. 27; *Heckmann,* K&R 2010, 770 (773) zur Bedeutung in vernetzten Zusammenhängen.

der Bürger ist. Deshalb kann auch ohne genaueren Blick auf die Ausführungen des Gerichts oder die Definitionsversuche der wissenschaftlichen Literatur zumindest eine Vorstellung von „informationstechnischen Systemen" vorausgesetzt werden.

Dem IT-System als *Datenkontext* wird mit der Schaffung des IT-Grundrechts eine neue Bedeutung beigemessen. Das betrifft aus staatlicher Sicht die Art der Datengewinnung[3] wie auch den Umgang mit den aus den Daten gewonnenen Informationen. Informationen sind durch ihre Datenbasis und durch deren Interpretation geprägt.[4] Bestimmend für das neue Schutzkonzept ist die besondere Qualität der auf Seite des Bürgers zugrunde liegenden Verarbeitungsstrukturen und -prozesse. Dementsprechend muss jede Bewertung bei der Bestimmung des IT-Systems und seiner Bedeutung für den Einzelnen ansetzen. Die Interpretationsebene wird jedoch insbesondere dann relevant, wenn sich die Risiken systemspezifischer Eingriffe auf die Interpretation der erlangten Daten auswirken können. Das ist etwa der Fall, wenn erhebliche Risiken einer Manipulation durch Dritte bestehen, die sowohl die Interessen des Betroffenen als auch der Ermittler beeinträchtigen.

Angesichts der von einer marktwirtschaftlichen Dynamik geprägten Entwicklung der Informationstechnologie muss ein wirksamer Grundrechtsschutz bereits zwingend die Technikgestaltung einbeziehen. Die Abwehr von Informationseingriffen in IT-Systeme ist damit nur *ein* Bestandteil eines umfassenden und mehrere Grundrechte übergreifenden Schutzkonzepts. Wichtig ist schon eine grundrechtswahrende Gestaltung von Systemen und Abläufen. Selbst im Hinblick auf konkrete Beeinträchtigungen darf der *Kontext* des Eingriffs nicht außer Acht gelassen werden. (Staatliche) Methoden müssen in allen Phasen auf die besonderen Anforderungen der IT-Systeme ausgerichtet werden. Damit ist freilich eine weitere Verrechtlichung verbunden, die aber mit der fortschreitenden Technisierung korrespondiert.

Die Formulierung „Vertraulichkeit und Integrität informationstechnischer Systeme" weist eine Reihe von Bedeutungsaspekten auf und vermittelt die trügerische Erwartung eines absoluten Schutzanspruchs. Schon grundlegende Erfahrungen mit dem Thema IT-Sicherheit lehren den durchschnittlichen Nutzer von Personal Computern, Smartphones und ähnlichen Geräten, dass

---

[3] S. zum unscharfen Begriff des Informationseingriffs etwa BVerfGE 65, 1 (52); *Schwan*, VerwA 66 (1975), 120 (127 ff.). Unter diesem Begriff wird missverständlich auch die Informationstätigkeit des Staates zusammengefasst, vgl. *Bethge*, in: Merten/Papier, Handbuch der Grundrechte, Bd. III, § 58 Rn. 42. Besser geeignet erscheint im Zusammenhang mit (staatlichen) Warnungen der Begriff des „Informationshandelns", vgl. BVerfGE 105, 252 (268).

[4] Vgl. *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts, Bd. II, 2. Auflage, § 22 Rn. 12, die für den Kontext weiter zwischen Daten, Beobachtungen und Mitteilungen differenziert.