

Schutz der Privatheit

Danilo Kardel

IT-Beratung und Management
dk@kardel-it.de

Auch wenn die Frage, was die Gesamtheit eines Menschen über seine Physis hinaus überhaupt ausmacht, gar nicht geklärt ist, kann seine Identität versuchsweise definiert werden als die Summe aller über ihn existierenden Informationen¹. Das Wesen der Information ist, „die implizite (latente, an sich vorhandene) Relation zwischen dem Einzelnen und dem Allgemeinen explizit zu machen“ (nach G. Werckmeisters Interpretation der Hegelschen Dialektik²).

Die informationelle Selbstbestimmung eines Individuums besteht darin, Produzent der Informationen über sich selbst zu sein, und verfügen zu können, wer Kenntnis von diesen Informationen erhält. Entsprechend beinhaltet die informationelle Fremdbestimmung sowohl die Produktion von Informationen über ein Individuum durch Andere („Identifizierung“) als auch die vom Individuum selbst nicht kontrollierbare Verwendung und Zuweisung von Informationen. Informationelle Fremdbestimmung erfolgt z.B. innerhalb der Gesellschaft (Einordnung in gesellschaftliche Gruppen oder Zuweisung eines sozialen Status), in der Arbeitswelt, auf staatlicher Ebene, oder automatisiert durch elektronische Datenverarbeitung. Dabei werden Identifizierungsmerkmale und Identifizierungsmethoden willkürlich durch Dritte festgelegt und mit personenbezogenen „gespeicherten“ Daten korreliert. Historische Beispiele für gesellschaftliche Gruppen, denen Menschen (auch) durch informationelle Fremdbestimmung zugeordnet wurden, sind „Zigeuner“ oder „Juden“. Aktuell findet informationelle Fremdbestimmung in besonderem Maße statt bei der Identifizierung von „Straftätern“ oder „Terroristen“, teilweise mit hohem Automatisierungsgrad. So kamen in den vergangenen Jahren hunderte von signature strikes der U.S. Army in ihrem war on terror zustande³. Die genannten Beispiele deuten bereits an, wie informationelle Fremdbestimmung für Individuen bedrohlich werden kann.

Informationelle Selbstbestimmung, d.h. die Befähigung des Individuums zur Kontrolle über Entstehung und Verbreitung von Informationen über sich selbst, ist das einzige Mittel gegen ein Übermaß an informationeller Fremdbestimmung. Wenn ein Individuum von seinem Recht auf informationelle Selbstbestimmung Gebrauch macht, entsteht Privatheit.

¹ W. Schmale, M. Tinnefeld, Privatheit im digitalen Zeitalter, Wien 2014.

² G. Werckmeister, DVR Band 7, 1978. <http://www.hegel-system.de/de/v131-werckmeister.htm>; Zugriff 20.05.2014.

³ Nach: <http://drones.procon.org/>; Zugriff 20.05.2014.

Privatheit hat es immer gegeben, auch wenn unser heutiger Privatheitsbegriff sich stark von den individuellen Optionen zur Schaffung von Privatheit in der Vergangenheit unterscheidet, etwa im Mittelalter oder in der Antike. Die Idee des „Gartens als Ort der Privatheit“ (M. Tinnefeld), in dem Menschen sich unkontrolliert bewegen können, begegnet uns bereits in den ältesten überlieferten Erzählungen. Beim Garten Eden allerdings haben wir es mit einem frühen Fall von totaler Überwachung zu tun: Bei Übertretung des (nur aus einem einzigen Verbot bestehenden) Gesetzes erfolgt umgehend die Abschiebung aus dem Paradies.

Privatheit ist von zentraler Bedeutung als Fundament einer anti-totalitären demokratischen Zivilgesellschaft. Ohne Privatheit und Privatsphäre gibt es keine Demokratie, ebenso wenig wie ohne Informationsfreiheit, Meinungs-, Presse- und Medienfreiheit. Privatheitsschutz und Datenschutz sind als besondere rechtskulturelle Leistungen anzuerkennen.

Die Vereinten Nationen haben im Jahre 1948 in der Allgemeinen Erklärung der Menschenrechte das Recht auf Privatheit (right to privacy) als eines der universellen Menschenrechte erkannt. Das Bundesverfassungsgericht hat 1983 erstmals ein Grundrecht auf informationelle Selbstbestimmung anerkannt, indem es dem Einzelnen das Recht gewährt, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“⁴ Die EU hat mit der Konvention zum Schutz der Menschenrechte und Grundfreiheiten aus dem Jahre 1950 (auch unter der Bezeichnung Europäische Menschenrechtskonvention, EMRK) und der EU-Grundrechte-Charta (EGRC, auch Charta der Grundrechte der Europäischen Union) von 2000 fortschrittliche Standards zum Datenschutz und zum Schutz der Privatsphäre geschaffen. Artikel 8 der EMRK lautet⁵:

(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

(2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Die EU-Grundrechte-Charta enthält je einen Artikel zum Schutz der Privatsphäre und zum Recht auf informationelle Selbstbestimmung. Artikel 7 der EGRC fordert die Achtung der Privatsphäre entsprechend EMRK, Art. 8 (s.o.); Artikel 8 der EGRC erklärt den Schutzbedarf personenbezogener Daten⁶:

⁴ BVerfGE 65, 1 – Volkszählung; Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983; zitiert nach: <http://www.servat.unibe.ch/dfr/bv065001.html#>; Zugriff 25.05.2014.

⁵ Zitiert nach: <http://conventions.coe.int/Treaty/ger/Treaties/Html/005.htm>; Zugriff 20.05.2014.

⁶ Zitiert nach: http://www.europarl.europa.eu/charter/pdf/text_de.pdf; Zugriff 20.05.2014.

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Während also das Recht auf Privatsphäre und informationelle Selbstbestimmung mittlerweile einen starken rechtlichen Schutz genießt, steht heute mit dem automatisierten Erstellen von Profilen und „Signaturen“ durch Auswertung digitaler Spuren (vor allem im Internet) ein globales und zugleich umfassendes Werkzeug für informationelle Fremdbestimmung zur Verfügung. Sowohl staatliche als auch privatwirtschaftliche Einrichtungen nutzen die damit entstandenen Möglichkeiten extensiv, erstere eher unter sicherheitspolitischen Aspekten, letztere zum Zwecke individualisierter Manipulation aus ökonomischen Interessen. Die Untersuchungen von Privacy International mit einem standardisierten „Privatsphären-Index“ zeigen bereits in den Jahren 2006 / 2007 bestürzende Ergebnisse über Ausmaß und Ausweitung weltweiter Überwachung⁷.

Um dem Anspruch gerecht zu werden, Privatheit und Privatsphäre als konstituierende Elemente einer anti-totalitären demokratischen Zivilgesellschaft zu schützen, ist es heute dringend erforderlich, Individualrechte zu stärken und bessere Kontrollfunktionen zu implementieren, die es dem Einzelnen ermöglichen, seine informationelle Selbstbestimmung zu behaupten bzw. wiederzuerlangen.

Bedingt durch den strukturellen Wandel der Arbeits-, Erwerbs- und Geschäftswelt und durch die Konvergenz bislang getrennter virtueller Handlungsräume erhalten virtuelle Identitäten zunehmende Bedeutung. Ein wesentlicher Baustein zur Erlangung informationeller Selbstbestimmung in der E-Society ist daher die Befähigung des Individuums zum Management virtueller Identitäten. Privatheit wird in der digitalen Welt gewährleistet durch die Autonomie und das Recht des Individuums, seine Identität innerhalb (und außerhalb) elektronischer Netze selbst zu bestimmen.

Der Schutz von Privatheit und Privatsphäre bedarf also rechtsverbindlicher Optionen auf Anonymisierung und Pseudonymisierung, ein Recht auf virtuelle Identitäten. Ein nutzergesteuertes Management virtueller Identitäten erlangt zentrale Bedeutung beim Schutz der Privatheit in einer demokratischen Informations- und Wissensgesellschaft.

Weitere wichtige Aspekte ergeben sich mit der Inkraftsetzung bzw. Wiedererlangung informationeller Selbstbestimmung gegenüber dem digitalen „Gedächtnis“ des Internet. Dazu gehört das Recht auf Vergessen (werden). Das diesbezügliche Urteil des Europäischen Gerichtshofes vom 13. Mai 2014, demzufolge der Suchmaschinenbetreiber

⁷ Privacy International, http://en.wikipedia.org/wiki/Privacy_International; Zugriff 20.05.2014.

Google Links zu personenbezogenen Daten unter bestimmten Bedingungen entfernen muss, weist in die richtige Richtung⁸. Die Rechte des Einzelnen gilt es, endlich mit Ernsthaftigkeit einzufordern und durchzusetzen. Das gleiche trifft zu für das in der EU-Grundrechte-Charta bestätigte Recht jeder Person, „Auskunft über die sie betreffenden erhobenen Daten zu erhalten“ oder für den Grundsatz, die Verarbeitung und Weitergabe von Daten sei nur „für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage“ erlaubt. Schon die oberflächlichste Gegenüberstellung von EU-Recht und „unbewusst gelebter“ Internet-Praxis enthüllt überdeutlich die Diskrepanz zwischen Anspruch und Wirklichkeit.

G. Werckmeister sieht durch die Entwicklung der Informationstechnologie den „Weg geöffnet für die allseitige (universelle) Entfaltung der Individuen (die Allgemeinheit des Einzelnen), für die freie Entfaltung der Persönlichkeit.“ Diese Perspektive zu wahren und nicht durch Kontrolle, Überwachung und Fremdbestimmung mithilfe ebendieser Technologien zerstören zu lassen, nimmt eine humane Nutzung moderner Informationstechnologie sich zum Ziel. Um den Prozess eines gemeinwohlorientierten sozialen Miteinanders zu gestalten, bedarf es aktiver Maßnahmen in Bildung und Ausbildung, Kunst und Kultur.

⁸ EuGH, Rechtssache C-131/12: <http://curia.europa.eu/juris/liste.jsf?language=de&num=C-131/12>; Zugriff 20.05.2014.