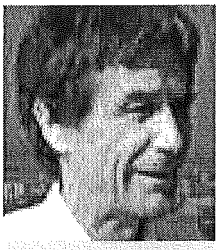
Der Ruf nach einem Recht auf Vergessen

Ein neues datenschutzbezogenes Verfassungsrecht im Spannungsfeld zwischen Privatheit und Transparenz?



Rolf H. Weber, Prof. Dr. iur., Ordinarius für Privat-, Wirtschafts- und Europarecht an der Universität Zürich, Visiting Professor an der Universität Hong Kong, Attorney-at-Law, Bratschi Wiederkehr & Buob, Zürich
rolf.weber@rwi.uzh.ch

Kürzlich ist in Europa der Ruf nach einem «Recht auf Vergessen» in der Online-Welt laut geworden. Materiell geht es um das Löschen von Datenspuren.

In den letzten Monaten ist im Kontext des Datenschutzes eine Diskussion über ein mögliches «Recht auf Vergessen», insbesondere mit Blick auf elektronische Datenspuren, aufgelebt. Der nachfolgende Beitrag geht den Grundlagen und Rahmenbedingungen eines solches «Grundrechts» nach.

Recht auf Vergessen – was ist gemeint?

Im Jahre 2010 haben erstmals Vertreter aus dem Umfeld der französischen Regierung den Gedanken geäussert, ein «Recht auf Vergessen» («right to be forgotten») sei für den Online-Bereich zu entwickeln (Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche[1]). In der Folge hat die EU-Kommission diesen Gedanken aufgenommen und vorgeschlagen, im Rahmen der Revision der Datenschutz-Richtlinie 95/46/EG auch vertieft über ein Recht auf Vergessen nachzudenken[2]. Seither erwähnen Vertreter der EU-Kommission ein solches neues Grundrecht vermehrt in öffentlichen Anhörungen und publizierten Stellungnahmen.

Das Konzept eines Rechts auf Vergessen ist nicht vollständig neu. Vielmehr wird schon seit einigen Jahren darüber diskutiert, ob es nicht angebracht sei, historische Ungerechtigkeiten zu «vergessen»; sachlich geht es darum, dass z.B. Rassendiskriminierungen oder Völkerrechtsverletzungen nach Ablauf einer (längeren) Frist nicht mehr zum Anlass für politische «Sanktionen» verwendet werden sollen[3]. Dieser Kontext betrifft indessen in der englischen Sprache das «right to forget», nicht das «right to be forgotten». Die erste Konstellation erfasst die aktive Seite des «Vergessens», indem historische Ereignisse nach Ablauf einer vernünftigen Periode keine Revitalisierung mehr erfahren dürfen, während die passive Seite in der zweiten Konstellation das Recht des Einzelnen abdeckt, persönliche Datenspuren zu löschen, damit Drittpersonen sie nicht mehr verfolgen können, d.h. ein Individualrecht, selber über das langzeitige Vorhandensein von persönlichen Informationen zu entscheiden[4].

Das Recht auf Vergessen befindet sich im Spannungsfeld zwischen dem Anliegen auf Privatheit und dem Erfordernis nach Transparenz. Nicht überraschend hat denn auch der US-Supreme-Court-Richter Louis Brandeis nicht nur (zusammen mit Samuel Warren) im Jahre 1890 den ersten ganz grundlegenden Beitrag zum Datenschutz als Ausfluss der Bewahrung der Individualsphäre auf Vertraulichkeit geschrieben («right to be let alone»[5]), sondern auch, insbesondere in öffentlichen Angelegenheiten, im Jahre 1914 vehement für Transparenz plädiert, und zwar mit dem bekannten kurzen Satz «Sunlight is said to be the best of disinfectants» [6].

Recht auf Vergessen und Persönlichkeitsrecht

Tragweite des Grundrechtschutzes

Das Recht auf Vergessen weist viele Elemente des durch Art. 28 ZGB geschützten Persönlichkeitsrechts auf. Schon seit Jahrzehnten räumt das Persönlichkeitsrecht den Individuen den Anspruch ein, gegen Verletzer der «Geheimsphäre» vorzugehen. Ursprünglich hat sich dieser Anspruch vornehmlich gegen die Medien gerichtet; mit der Verbreitung des Internets hat das Persönlichkeitsrecht insoweit aber eine klare Erweiterung des Anwendungsbereichs erfahren[7].

Das Persönlichkeitsrecht ist bereits vielfach Grundlage bundesgerichtlicher Entscheide gewesen, welche die Privatsphäre von Individuen geschützt haben. Besonders augenfällig hat das Bundesgericht im Jahre 1944 mit Blick auf ein Bild «Hodler auf dem Sterbebett» dafür gehalten, die Pietätsgefühle der Witwe Hodler würden das Interesse des Malers an der Ausstellung dieses Bildes in einer Galerie überwiegen[8]. In weiteren Fällen ist es darum gegangen, dass Informationen mit strafrechtlich relevantem Hintergrund viele Jahre später der Öffentlichkeit nicht mehr be-

kannt gemacht werden sollten; abhängig von den konkreten Umständen und der Schwere der früheren Tat hat die Gerichtspraxis anerkannt, dass ein Recht des Verurteilten auf Vergessen durchaus bestehen könne; die Länge der Zeitspanne zwischen einer strafrechtlich relevanten Tat und der späteren Veröffentlichung der Verurteilung hängt selbstredend von den konkreten Gegebenheiten ab[9]. Die Grundbotschaft ist aber klar: Früher transparent gemachte Informationen werden gegebenenfalls «informationsunwürdig», wenn das Interesse der Öffentlichkeit daran gering geworden ist und eine erneute Publikmachung das betroffene Individuum stark beeinträchtigen könnte.

Ähnliche rechtliche Diskussionen werden auch in anderen Ländern geführt, etwa in Deutschland mit Bezug auf Personen, die während des 2. Weltkrieges oder in der Deutschen Demokratischen Republik ein strafrechtlich relevantes Verhalten an den Tag gelegt haben, das Jahrzehnte später nicht neu aufgerollt werden sollte, oder in Spanien, wo Google von der spanischen Datenschutzbehörde wegen behaupteter Verletzung des Rechts auf Vergessen eingeklagt worden ist[10]. Nach den bekannten, die Privatsphäre von «öffentlichen» Persönlichkeiten schützenden Urteilen (z.B. Caroline von Hannover) hat auch der Europäische Menschenrechtsgerichtshof im Jahre 2009 dafür gehalten, dass die Publikation einer früheren strafrechtlichen Verurteilung die Ehre und Reputation der betroffenen Person besonders stark in Mitleidenschaft gezogen sowie die moralische und psychologische Integrität beeinträchtigt habe[11]; die Urteilserläuterungen basieren zwar auf allgemeinen Datenschutzüberlegungen, nicht auf dem Recht auf Vergessen, doch ist die Begründungslage sehr ähnlich.

Beschränkungen des Grundrechtschutzes

Nach international weitgehend vergleichbaren Rechtsgrundsätzen vermag die betroffene Person in eine Datenbearbeitung und Datensammlung einzuwilligen (Art. 13 Abs. 1 DSG). Schwierig ist aber oft die konkrete Abwägung der Tragweite einer solchen Einwilligung. International bekannt geworden ist der Fall von Stacy Snyder, einer US-Studentin der Pädagogik, die Lehrerin werden wollte und ein Bild von ihr, aufgenommen an einem sozialen Anlass, auf MySpace platzierte; dieses Bild zeigte sie alkoholtrinkend mit einem Plastikglas und einem Piratenhut. Bei einer späteren Bewerbung wurde Stacy abgelehnt, und zwar mit der Begründung, ihr Verhalten als «drunken pirate» sei unprofessionell und würde die junge Generation zum Alkoholgenuss verleiten[12]. Der Versuch, diesen Entscheid vor Gericht aufzuheben, und zwar gestützt auf die Meinungsäusserungsfreiheit, scheiterte[13]. Selbstredend bleibt insoweit die Frage im Raum, ob Stacy mit dem Hochladen ihrer Foto die Einwilligung zu deren Verwendung in einem späteren Bewerbungsverfahren gegeben habe; individuell betrachtet dürfte dies regelmässig nicht der Fall sein, doch lässt sich argumentieren, wer ein Foto in einem sozialen Netzwerk publiziere, müsse damit rechnen, dass eine Bezugnahme darauf später auch in einem anderen Kontext möglich sei.

Früher transparent gemachte Informationen werden «informationsunwürdig», wenn das Interesse der Öffentlichkeit daran gering geworden ist.

Eine weitere Beschränkung des Grundrechtschutzes kann sich aus öffentlichen Interessen ergeben (Art. 13 Abs. 2 DSG). Der Staat mag interessiert sein, zum Zwecke der Gewaltprävention z.B. Informationen über Hooligans bekannt zu machen. Jedes staatliche Handeln, das einen Grundrechtseingriff bewirkt, steht dabei unter dem Vorbehalt der Anwendung des Verhältnismässigkeitsprinzips; Personendaten sind zu löschen, wenn sie zur Erfüllung der öffentlichen Aufgabe nicht mehr gebraucht werden[14].

Möglicher Inhalt eines neuen Rechts auf Vergessen

Komplexes Konzept der Privatheit

Das Internet und die neue virtuelle Welt haben die Möglichkeiten zum Anlegen von Datenspuren vervielfacht. Traditionelle Datenschutzkonzepte vermögen mit den neuen Herausforderungen nicht mehr Schritt zu halten. Aus diesem Grunde erscheint es als unumgänglich, die Privatheit durch einen multi-dimensionalen Ansatz, der physische, psychologische, transaktionale und soziale Elemente mitumfasst, ausreichend zu schützen; ins-

Kurz & bündig

Das neu auf europäischer Ebene postulierte «Recht auf Vergessen» will dem Einzelnen das Recht einräumen, Daten auf dem Internet «zum Verschwinden» zu bringen. Die Risiken für die Privatheit sind im Internet unübersehbar; die Sensibilität mit Bezug auf vorhandene Datenspuren ist deshalb zutreffend gewachsen. Die gegenwärtige Diskussion erweist sich aber noch als zu vage: Die Schaffung eines neuen Grundrechts allein genügt nicht, vielmehr bedarf es der Erörterung der notwendigen technischen und rechtlichen Konkretisierungen hinsichtlich des Löschens von Daten, d.h., ein neues Grundrecht erfordert die konkrete Umsetzung in ein spezifisches Anspruchssystem.

besondere die soziale Dimension, d.h. die Fähigkeit, soziale Interaktionen zu kontrollieren, bedarf einer verstärkten Betrachtung[15].

Folgende fünf Formen von Privatheit lassen sich konkretisieren und analysieren[16]:

Informationeller Datenschutz betrifft letztlich die autonome Kontrolle über die Information.

- Relevant ist vorerst die Kontrolle über den individuellen Informationsfluss, der die Risiken einer möglichen Privatheits-Invasion determiniert.
- Privatheit betrifft auch die Freiheit von Eingriffen in und Kontrolle über Informationsvorgänge.
- Gesetzgeberisch festzulegen ist weiter der Bereich des Privatheitsschutzes und damit der Unverletzbarkeit der Vertraulichkeit.
- Privatheit bedeutet überdies das Recht, «allein zu sein».
- Der technische Schutz vor Dritteingriffen in die Privatheit ist zu gewährleisten.

Aus diesen Überlegungen entsteht ein «Cluster» von Datenschutzmassnahmen, der eine starke Bezugnahme auf die Autonomie des Individuums in der Gestaltung der persönlichen Informationsversorgung aufweist. Informationeller Datenschutz betrifft letztlich die autonome Kontrolle über die Information[17].

Individualisierung des Schutzkonzepts

Wie erwähnt ist die Autonomie des Individuums ein zentrales Element des Datenschutzes. Konkret bedeutet diese Erkenntnis, dass ein mehr individuenbezogener Ansatz der datenschutzrechtlichen Betrachtungsweise als angebracht erscheint[18]. Argumentationsansätze sind im geltenden Recht durchaus vorhanden:

- Zu denken wäre z.B. an die Lizenzanalogie, indem der Verfügungsmacht über Information ein eigentumsähnlicher Charakter zuerkannt wird[19], der es ermöglicht, «Gebrauchsbedingungen» aufzustellen; dazu könnte die Anordnung gehören, dass gewisse grundsätzlich verfügbare Informationen nur während einer bestimmten Zeit in Anspruch genommen werden dürfen.
- Informations-Privatheit lässt sich auch funktionell verstehen, und zwar unter dem Aspekt des öffentlichen Wertes der Information («public value»); aus dieser Perspektive zeigt die Informations-Privatheit die Charakteristiken eines öffentlichen Gutes, das einen bestimmten Grad an sozialer und rechtlicher Kontrolle ermöglichen muss[20].

Fussnoten

1 <http://www.aidh.org/Actualite/Act_2010/Images/Charte_oubli_La_Charte.pdf>.
2 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609 endg., 4. November 2010.
3 Gregory W. Streich, Is There a Right to Forget? Historical Injustices, Race, Memory, and Identity, New Political Science, Vol. 24/4, 2002, 525–542.
4 Vgl. Rolf H. Weber, The Right to be Forgotten – More than a Pandora's Box?, JIPITEC 2011, 120 f., Rz. 3.
5 Samuel D. Warren/Louis D. Brandeis, The Right to Privacy, Harvard Law Review, Vol. 4, 1890, 193–220.
6 Louis D. Brandeis, What Publicity Can Do, in: Other People's Money: And How the Bankers Use It, New York 1914, 92.
7 Vgl. Julia Meyer, Identität und virtuelle Identität natürlicher Personen im Internet, Baden-Baden 2011.
8 BGE 70 II 127.
9 BGE 104 II 225, E. 5b; BGE 122 III 449; BGE 5C.156/2003 vom 23. Oktober 2003; Franz Werro, The Right to Inform v. the Right to be Forgotten: A Transatlantic Crash, in: Liability in the Third Millennium, Liber Amicorum Gert Brüggemeier, Baden-Baden 2009, 285 ff.
10 <http://www.bbc.co.uk/news/technology-12239674>.
11 EMGR, A. v. Norway, 9. April 2009, No. 28070/06, Sect. 1.
12 Vgl. Viktor Mayer-Schönberger, delete. The Virtue of Forgetting in the Digital Age, Princeton/Oxford 2009, 1–3.
13 <http://voices.washingtonpost.com/securityfix/Decision%20 2008.12.03.pdf>.
14 Bruno Baeriswyl, Datenschutz in der Verwaltung, in: Weber et al., Datenschutz im europäischen Umfeld, Zürich 1995, 161, 171.
15 Vgl. Weber (Fn. 4), 125, Rz. 30.
16 Hayden Ramsay, Privacy, Privacies and Basic Needs, The Haythrop Journal, Vol. 51, 2011, 288–297.
17 Ulrike Hugl, Approaching the Value of Privacy: Review of theoretical privacy concepts and aspects of privacy management, AMICIS 2010 Proceedings, Paper 248, 4.
18 Vgl. Rolf H. Weber, How does Privacy Change in the Age of Internet, in: Christian Fuchs/Kees Boersma/Anders Albrechtslund/Marisol Sandoval (Hrsg.), Internet and Surveillance: The Challenges of Web 2.0 and Social Media, Oxford 2011, 273 ff.
19 Paul M. Schwartz, Property, Privacy, and Personal Data, Harvard Law Review, Vol. 117, 2004, 2055 ff.
20 Vgl. auch Colin J. Bennett/Charles D. Raab, The Governance of Privacy. Policy Instruments in Global Perspective, Cambridge Mass./London 2006, 29 ff.
21 Eingehend dazu Mayer-Schönberger (Fn. 12), 128 ff.
22 Mayer-Schönberger (Fn. 12), 144 ff.
23 Mayer-Schönberger (Fn. 12), 169 ff.
24 Weber (Fn. 4), 127, Rz. 36.
25 <http://www.huntonprivacyblog.com/2010/10/articles/european-union-1/french-government-secures-right-to-be-forgotten-on-the-internet/>.
26 Vgl. schon Rolf H. Weber, Datenschutzrecht vor neuen Herausforderungen, Zürich 2000, 75.
27 Vgl. Rolf H. Weber, digma 2008, 94 ff.

Konturen eines Grundrechts

In seiner 2009 publizierten bekannten Schrift «delete» hat MAYER-SCHÖNBERGER sieben potenzielle (teilweise rechtliche) Konzepte entwickelt, welche die Schwächen des «digitalen Gedächtnisses» zumindest mildern sollten[21]. Nur beschränkt rechtlich ausgerichtet sind die Ansätze der digitalen Abstinenz, der kognitiven Anpassung an die neuen Gegebenheiten, der angemessenen Kontextualisierung der vorhandenen Informationen sowie allgemein der Informationsökologie, obwohl alle vier Ansätze in der sich entwickelnden Informationsgesellschaft von grosser Bedeutung sind. Mit besonderer rechtlicher Relevanz ausgestattet sind hingegen eigentumsähnliche informationelle «Privatheitsrechte», wie sie bereits mit Hinweis auf die Lizenzanalogie angesprochen wurden; im Einzelnen stellen sich dann z.B. Fragen der verfahrensmässigen Vorgehensweise und der Beweislast. Überdies liesse sich daran denken, eine digitale Privatheits-Infrastruktur zu schaffen, und zwar etwa so, wie insbesondere audiovisuelle Medien dies mit dem Digital Rights Management (DRM) getan haben: Anzustreben wäre dabei nicht der Schutz des Urheberrechts, sondern der Schutz der privaten Information[22]. Ein solches System weist aber ähnliche Nachteile auf wie die DRM-Systeme, die sich eigentlich nicht durchgesetzt haben.

Am eingehendsten erläutert MAYER-SCHÖNBERGER das Konzept von Verfalldaten für digitale Informationen[23]. In einem solchen Konzept, das technisch durchaus realisierbar ist, würden die Informationsprozessoren eine zentrale Rolle erhalten; komplexe Technologien sind von den Individuen nicht zu handhaben, sondern materiell geht es vielmehr darum, dass sachgerechte Verfalldaten gesetzt werden. In gewissen Konstellationen ist es auch denkbar, die Verfalldaten auszuhandeln, insbesondere in vertraglichen Kontexten. Gewisse Schwächen lassen sich immerhin nicht übersehen, z.B. Fragen wie die Verantwortung für das Löschen von Informationen oder die Anpassung von Verfalldaten bei veränderten Umständen[24].

«Wert» eines neuen Grundrechts

Die Proklamation eines neuen Grundrechts allein verstärkt die Schutzposition des Individuums (noch) nicht. Vielmehr hängt die konkrete Ausgestaltung des Individualschutzes von der Konkretisierung des Schutzkonzepts ab, wie sie etwa durch Richtlinien oder Verhaltensleitlinien zu erfolgen vermag (z.B. Code of Good Practice on the Right to be Forgotten on Social Networks and Search Engines)[25]. Ein Recht auf Vergessen muss also durch die rechtlichen Instrumente, welche die Individuen und Unternehmen lernen, wie Datenschutzprinzipien auf der Basis der privatheitsbezogenen Autonomie anzuwenden sind, ergänzt werden. Dabei lässt sich nicht übersehen, dass technische Massnahmen regelmässig schneller eingeführt sind als rechtliche Normen[26].

Im Anschluss an das vom Deutschen Bundesverfassungsgericht mit Urteil vom 27. Februar 2008 geschaffene «Computergrundrecht» auf Vertraulichkeit und Integrität[27] müsste das Recht auf Vergessen dem Individuum nicht nur die Möglichkeit zuerkennen, seine Beziehungen frei und selbstverantwortlich zu gestalten, sondern sich auch gegen die Herstellung einer staatlichen oder privaten Öffentlichkeit zu wenden und die Publikmachung von Informationen zu verbieten, solange es an einem sachbezogenen Einverständnis fehlt. Von Bedeutung wäre dabei, dass ähnlich dem zwar von der Sache her nicht identischen «Computergrundrecht» sich auch aus dem Recht auf Vergessen spezifische Ansprüche ableiten liessen, welche die Inhaber von Informationen in die Pflicht nehmen, nach Ablauf des angeordneten oder sich aus den Umständen ergebenden Verfalldatums von einer weiteren Zugänglichmachung solcher Informationen abzusehen. Konkret müsste es darum gehen, dass ein Individualrecht den Anspruch auf Anwendung technischer Massnahmen zur Sicherstellung der Privatheit miteinschliessen würde. Die Bemühungen der EU-Organe um das Recht auf Vergessen scheinen sich derzeit auf ein moralisches Postulat zu beschränken; einen datenschutzrechtlichen Gewinn würde ein neues Grundrecht aber nur bringen, wenn eine Umsetzung in ein konkretes Anspruchssystem gelingt. ■

Einen datenschutzrechtlichen Gewinn würde ein neues Grundrecht nur bringen, wenn eine Umsetzung in ein konkretes Anspruchssystem gelingt.