Göttrik Wewer

Auf dem Weg zum gläsernen Staat? Privatsphäre und Geheimnis im digitalen Zeitalter

Zusammenfassung
Die Grenzlinie zwischen Privatsphäre und Öffentlichkeit ist nicht starr, sondern hat sich im Laufe der Geschichte immer mal wieder verschoben. Gegenwärtig ist eine merkwürdige Koalition aus kommerziellen „Datenfressern" wie *Facebook, Google & Co.* und auch Netzaktivisten mit der Parole unterwegs, das Zeitalter der Privatsphäre sei nunmehr vorbei. Während die einen am „gläsernen Bürger" arbeiten, zielen die anderen auf einen „gläsernen Staat". Danach würden Staat und Verwaltung nicht nur ihre Datenbestände für kommerzielle Nutzungen bereitstellen („*Open Data"*) und „soziale Medien" im Web 2.0 nutzen („*Open Government"*), sondern letztlich ganz auf vertrauliche Informationen und Geheimnisse verzichten sollen („totale Transparenz"). Plattformen wie *WikiLeaks* haben sich darauf spezialisiert, staatliche Geheimnisse aufzudecken; die Bediensteten werden offen ermuntert, ihre Verschwiegenheitspflicht zu ignorieren und Dienstgeheimnisse auszuplaudern („*Whistleblowing"*). Nur so ließen sich Machtmissbrauch und Korruption eindämmen. Wenn sich diese Ideologie totaler Transparenz durchsetzen würde, stünde am Ende eine weitere Schwächung des demokratischen Staates: gegenüber den Internetriesen, die ihre eigenen Daten und Strategien keineswegs offenlegen, und gegenüber diktatorischen Regimes, in denen das staatliche Geheimnis alles gilt und das private Geheimnis nichts. Aber auch die Gesellschaft würde sich massiv verändern, wenn das Spannungsfeld von Privatheit und Öffentlichkeit sowie Geheimnis und Verrat nicht mehr in der politischen Auseinandersetzung jeweils immer neu ausbalanciert, sondern in totaler Transparenz aufgelöst würden: keine Privatheit mehr, keine Geheimnisse mehr. Die Frage ist, ob das ein erstrebenswertes Gesellschaftsmodell oder ob es an der Zeit ist, Einhalt zu rufen.

Abstract
Welcome, big glassy state?
Privacy and secrecy in the digital age
The borderline between the private and the public is not a fixed one, and it has shifted from time to time during the course of history. Presently, a strange coalition of commercial "data guzzlers" like Facebook, Google etc and Internet activists try to assure us that the age of privacy is now over. While the former are working to achieve a "transparent citizen", the latter aim for a "transparent state". According to that concept, state and administration should not only offer their data for commercial use ("open data") and use "social media" in the Web 2.0 ("open government"), but they should ultimately completely forego confidential information and secrecy ("total transparency"). Organisations like WikiLeaks have specialised in uncovering state secrets; public employees are openly encouraged to ignore their duty of silence and to publicise official secrets ("whistleblowing"). The underlying argument is that this is the only way to rein in abuse of power and corruption. If this ideology of total transparency were to become dominant, this could well result in a further weakening of the democratic state, both with regard to corporate giants on the Internet (who do not publicise their own data and strategies) and to dictatorial regimes (who treasure secrecy and scorn privacy). But society would also change massively, if the tension between the private and the public as well as between secrecy and treason need no longer be discussed and rebalanced in political discourse, but would be resolved once and for all for total transparency: there would be no more privacy, and no more secrets. It is questionable, whether this would be a desirable model of society, or whether it is time to call for an end of that debate.

dms – der moderne staat – Zeitschrift für Public Policy, Recht und Management, 5. Jg., Heft 2/2012, S. 247-262

Schlagworte: Privatsphäre, Öffentlichkeit, Dienstgeheimnis, Geheimnisverrat, totale Transparenz, gläserner Staat

Key words: privacy, publicity, official secrets, treason, total transparency, Big glassy state

1. Eine neue Ideologie totaler Transparenz

Am Abend des 18. September 2011 ereignete sich in Berlin eine kleine politische Sensation: Die Partei „Die Piraten", erst fünf Jahre zuvor gegründet, zog mit 8,9 Prozent der Stimmen und 15 Mandaten in das Berliner Abgeordnetenhaus ein (*Hirscher* 2011). Dass eine Partei, die vorher kaum jemand wahrgenommen hatte und die zu diesem Zeitpunkt gerade 12.000 Mitglieder zählte (aktuell: 22.000, in Berlin: 2.700), schon in ein Landesparlament einziehen konnte, hatte es zuvor nur selten gegeben (*Zolleis/Prokopf/Strauch* 2010, S. 5). Bei künftigen Bundestagswahlen wurden der jungen Partei manchmal schon zehn Prozent der Wählerstimmen oder sogar mehr zugetraut. Inzwischen sind die Piraten auch in die Landtage des Saarlandes (7,4 %, 4 Sitze), von Schleswig-Holstein (8,2 %, 6 Sitze) und Nordrhein-Westfalen (7,9 %, 20 Sitze) eingezogen.

Die neue Partei artikuliert das Lebensgefühl und das Weltverständnis jener Generation, die mit dem Computer und mit dem Internet groß geworden ist, und sie sammelt den Verdruss derjenigen ein, die mit CDU, SPD, Grünen, FDP und den Linken unzufrieden sind (*Häusler* 2011, S. 10). Längst nicht alle, die sie gewählt haben, können souverän mit dem Rechner umgehen oder interessieren sich für Netzpolitik. Die Piraten sind vielmehr eine bunte Mischung aus Netzpartei, Generationenpartei und Protestpartei (vgl. auch *Stoye* 2012). Selbst mit zehn Prozent der Wählerstimmen kann man nicht die Politik bestimmen, aber immerhin einer verbreiteten Unzufriedenheit und der Netzgemeinde eine Stimme in der politischen Diskussion geben. Die Bedeutung der Piraten für die politische Landschaft liegt vor allem darin, dass sie mit ihrem Stimmenanteil bestimmte Koalitionen („rot-grün" oder „schwarz-gelb") künftig unmöglich machen (können) (*Bieber* 2012). Ihr Einzug in die Parlamente könnte insofern einen Zwang zu Großen Koalitionen bewirken. Und die Wahlerfolge der Piraten bedeuten eine weitere Zersplitterung der Stimmen links von der Mitte (*Hirscher* 2011, S. 5).

Auf viele Fragen haben die Piraten keine Antwort. Das geben sie auch offen zu (man wolle sich „auf die im Programm genannten Themen konzentrieren"). Auch die anderen Parteien hätten auf viele Fragen keine wirklichen Antworten parat, sagen sie und verweisen auf die Eurokrise. Sie glauben aber daran, durch eine ständige Rückkopplung an die Basis über das Internet beliebig Antworten finden zu können („Schwarmintelligenz"), und vor allem daran, durch vollständige Transparenz dessen, was die gewählten Vertreter tun, einen neuen politischen Stil, eine neue Kultur zu praktizieren. Undurchsichtige Entscheidungen, Absprachen in „Hinterzimmern" und Einfluss der Lobby wollen sie nicht („irgendwas mit Internet und Transparenz"). Sie setzen sich für ein bedingungsloses Grundeinkommen, für freie Fahrt im öffentlichen Nahverkehr und für die Legalisierung weicher Drogen ein (*Schilbach* 2011). Seinen Beitrag zahlen muss man auch nicht unbedingt; das machen (im Juni 2012) nur 56,6 % der Mitglieder. Man kann Mitglied bleiben, ohne zu zahlen, darf dann aber nicht mit abstimmen.

Für die Entscheidung, Piraten zu wählen, scheint die Programmatik nicht so wichtig zu sein: Das Programm im Saarland war erst vierzehn Tage vor der Wahl überhaupt fertig – was nicht dafür spricht, dass viele Wähler es kennen konnten – und in Schleswig-

Holstein übernahmen die Piraten große Teile ihres Programms einfach aus Baden-Württemberg („Copy & Paste“) – obwohl vieles davon für das Land im Norden gar nicht passte. Als das auffiel, wurde es schnell repariert. Einer anderen Partei hätten das die Wähler sicher nicht so einfach durchgehen lassen. Das gilt auch für verbale Entgleisungen einzelner Mitglieder (z.B. Frauenförderung als „Tittenbonus“).

Es hat schon einmal eine Partei gegeben, die alles öffentlich verhandeln wollte: Die Grünen. Sie haben aber lernen müssen, dass Wähler Streit nicht unbedingt goutieren, dass bei „Schlachtfesten“, die auf offener Bühne zelebriert werden, immer auch Verletzte zurückbleiben und dass zur Politik auch vertrauliche Sondierungen gehören.

Die Piraten wollen das alles noch einmal ausprobieren. Im digitalen Zeitalter ergeben sich aus ihrer Sicht mit Instrumenten wie *Liquid Democracy*, *Adhocracy* oder dem Piratenwiki neue Chancen für Teilhabe und Transparenz, die es vorher so nicht gegeben hat. Man brauche kein Programm, heißt es, weil es genüge, ein Betriebssystem zu sein (*Häusler* 2011, S. 54). Das Credo der Piraten lautet: Wo das Internet ist, ist Demokratie nicht mehr zu unterdrücken (ebenda, S. 119).

Wir alle haben unsere kleineren und größeren Geheimnisse, von denen wir nicht möchten, dass andere sie erfahren. Das gilt für den einzelnen Menschen, für soziale Beziehungen, für Organisationen und für Institutionen, für Unternehmen wie für Ministerien. Die Welt ist voller Geheimnisse und noch immer voller Rätsel. Bei Geheimnissen handelt es sich um sensible Informationen, die anderen, für die sie durchaus von Interesse sein könnten, nicht bekannt sein sollen, die für sie nicht einsehbar sind.

Wenn Menschen, denen wir ein Geheimnis anvertraut haben, dieses verraten, dann können wir ihnen die Freundschaft kündigen oder die Scheidung einreichen. Wer Betriebsinterna ausplaudert oder Staatsgeheimnisse verrät, muss mit Strafe rechnen. Während das Betriebsgeheimnis technische Aspekte der Produktion umfasst, meint Geschäftsgeheimnis kaufmännische Aspekte. Beim Verrat von Geschäfts- und Betriebsgeheimnissen droht eine Freiheitsstrafe bis zu drei Jahren oder eine Geldstrafe, in besonderen Fällen sogar eine Freiheitsstrafe bis zu fünf Jahren (§ 17 UWG). Verrat ist ein besonders schwerer Vertrauensbruch, der die angenommene Loyalität verletzt.

Für staatliche Geheimnisse gibt es unterschiedliche Geheimhaltungsstufen. Über das „normale“ Amts- und Dienstgeheimnis hinaus sind das die Stufen: Vertraulich, Geheim, Streng Geheim („Verschlusssache – Nur für den Dienstgebrauch“). Wer solche Geheimnisse offenbart, muss ebenfalls mit Strafe rechnen. Die Aufgabe des strafrechtlichen Staatsschutzes (§§ 80–92 b StGB) besteht darin, den Bestand des Staates, seine Sicherheit und die verfassungsmäßige Ordnung zu schützen. Dabei unterscheidet man traditionell zwischen Hochverrat und Landesverrat: „Der erstere bezieht sich auf jede Straftat, die sich gegen den inneren Bestand des Staates, also gegen die Staatsverfassung, die Staatsgewalt oder das Staatsoberhaupt richtet, während Landesverrat alle Handlungen kriegerischen und nichtkriegerischen Charakters umschließt, die die äußere Sicherheit des Staates berühren“ (*Boveri* 1976, S. 780).

Der Gegensatz zu Geheimnis ist nicht Bekanntmachung, Offenbarung oder Transparenz, sondern Verrat. Eine Gesellschaft, in der Indiskretion, Illoyalität und Verrat zu leitenden Prinzipien würden, statt rechtlich und moralisch geächtet zu sein, könnte kaum funktionieren. Sie wäre von einer „Kultur des Misstrauens“ durchsetzt. *Margret Boveri* hat in ihren Studien zum „Verrat im 20. Jahrhundert“ einerseits darauf hingewiesen, dass aller radikale politische Wechsel mit Verrat anhebe, aber andererseits auch festgehalten: „Verrat ist Vertrauensbruch“ (*Boveri* 1976, S. 779).

Privatheit meint mehr als die kleineren und größeren Geheimnisse, die wir alle mit uns herumtragen. Sie meint eine Sphäre, in die wir uns zurückziehen können und die niemanden – außer vielleicht die Familie und die Freunde – etwas angeht – besonders den Staat nicht, aber auch die Wirtschaft und die Gesellschaft nicht. Die amerikanischen Juristen *Samuel Warren* und *Louis D. Brandeis* haben schon 1890 Privatheit als das Recht definiert, von anderen in Ruhe gelassen zu werden („the right to be let alone" [*Scherz/Höch* 2011, S. 20]).

Das Gegenteil von Privatheit ist Öffentlichkeit. Wer sich in der Öffentlichkeit bewegt, muss damit rechnen, beobachtet zu werden; wer sich in die Privatsphäre zurückzieht, will das gerade nicht: „Hier bin ich Mensch, hier darf ich's sein" (*Goethe*, Faust I, Vers 4610). Hier kann er seinen Gefühlen – wie Angst, Scham oder Ärger – freien Lauf lassen, ohne sich rechtfertigen zu müssen, hier kann er seine Bedürfnisse ausleben. Zur Würde des Menschen gehört das Recht, frei darüber befinden zu können, ob und wie er in der Öffentlichkeit stattfinden will (*Scherz/Höch* 2011, S. 23f.).

Die Grenzlinie zwischen Privatsphäre und Öffentlichkeit ist nicht starr, sondern verändert sich im Laufe der Geschichte: weil sich die sozialen Normen wandeln, wie man sich zu verhalten hat, und weil es neue technische Möglichkeiten gibt, die Privatsphäre zu durchlöchern. Sie ist auch nicht eindeutig markiert, sondern zwischen „öffentlich" und „privat" gibt es eine breite Grauzone. Diese Grauzone besser auszuleuchten, darum drehte sich immer der Streit um die Frage, was noch als private Angelegenheit gelten kann und was schon eine öffentliche Angelegenheit ist. Diese Frage müssen die Medien jeden Tag für sich beantworten, wenn sie etwas über Prominente erfahren; diese Frage muss aber auch die Gesellschaft immer wieder neu für sich beantworten. In der Bonner Republik galt als *common sense*, über die Geliebte eines verheirateten Politikers nicht zu berichten, sondern nur über Verfehlungen im öffentlichen Amt. In der Berliner Republik müssen Politiker damit rechnen, auch in ihrem Privatleben regelrecht ausspioniert zu werden (*Scherz/Höch* 2011, S. 16). Seit es Internet gibt, *YouTube* und Handy-Cameras, mit denen jeder schnell ein Bild machen kann, können sich Prominente kaum noch ungestört bewegen.

Bei allem Streit war doch bisher klar, dass es so etwas wie eine Privatsphäre geben muss, wenn der Mensch als Mensch existieren will, und dass Verrat sich nicht gehört und geahndet werden muss. Eine *totale* Öffentlichkeit hat jedenfalls bis vor wenigen Jahren noch niemand gefordert, auch wenn öfter vehement um *mehr* Öffentlichkeit gestritten wurde („auch das Private ist politisch"). Und dass Unternehmen ihre Planungen, Entwicklungen und Innovationen schützen und auch der Staat gewisse Informationen vertraulich behandelt, war nicht grundsätzlich umstritten. Jedenfalls wurde nicht offensiv dafür geworben, Betriebsinterna und Staatsgeheimnisse auszuplaudern. Allenfalls gab es im Einzelfall ein gewisses Verständnis, bestimmte Interna öffentlich gemacht zu haben („Pentagon-Papiere", *Watergate*). In diesen Fällen handelte es sich jedoch um eine bewusste Irreführung der Öffentlichkeit durch Amtsträger oder eindeutig um Machtmissbrauch. Für Illoyalität und Verrat gab es jedenfalls hohe moralische Hürden.

Dieser Grundkonsens scheint inzwischen ins Wanken zu geraten. „*The age of privacy is over*", verkündet zum Beispiel kurz und bündig *Facebook*-Gründer Mark Zuckerberg (zitiert nach *Scherz/Höch* 2011, S. 5). Privatheit gebe es künftig schlicht nicht mehr. Und Julian Assange, der Gründer von *WikiLeaks*, versteht seine Plattform als eine soziale Bewegung zur Aufdeckung von Geheimnissen (insbesondere von Regierungen, von westlichen Regierungen) (*Rosenbach/Starck* 2011). „Kollateralschäden", also Gefahren für

Leib und Leben unschuldiger Menschen, werden bei dem Streben nach *totaler Transparenz* in Kauf genommen: Hauptsache, keine Geheimnisse mehr (*Khatchadourian* 2011, S. 11ff., hier S. 41).

Es ist eine merkwürdige Koalition von kommerziellen „Datenfressern" wie *Facebook, Google & Co.* (*Kurz/Rieger* 2011) und *Hackern* wie Assange, die sich anschickt, wesentliche Koordinaten unserer Demokratie zu verschieben. Während die einen primär den „gläsernen Bürger" ins Visier nehmen, aber auch gerne staatliche Daten ausbeuten würden *(„Open Data")*, zielen die anderen vorrangig auf den „gläsernen Staat". Dass beide selbst nicht sehr transparent agieren und sich nur ungern in die Karten gucken lassen, gehört zur Ironie der Geschichte. Das Spannungsfeld von Privatheit und Öffentlichkeit und von Geheimnis und Verrat, in dem wir uns bisher bewegt haben, würde sich jedenfalls deutlich verändern: Keine Geheimnisse mehr, keine Privatheit mehr. Es droht die totale Transparenzgesellschaft (*Han* 2012b).

Im Folgenden soll gefragt werden, welche Positionen die Piraten in dieser Debatte vertreten und wie sich diese von anderen Auffassungen in der Netzgemeinde unterscheiden. Dabei geht es zunächst um die Privatheit des Bürgers (2.) und dann um Geheimnisse des Staates (3.). Würde es gelingen, „den Staat nackig zu machen", dann würden sich – so die These – die Gewichte zwischen Wirtschaft und Staat, aber auch zwischen Demokratien und Diktaturen weiter zu seinen Ungunsten verschieben (4.). *Totale Transparenz* (nur) von Bürger und Staat ist jedenfalls kein erstrebenswertes Ziel. Die Diskussion darüber hat noch kaum begonnen. Es wird Zeit, sich einzumischen.

2. Ist Privatheit des Menschen *out*?

Die Ursprünge der Piraten gehen zurück auf die „*Declaration of the Independence of Cyberspace*", die *John Perry Barlow* formuliert hat (siehe unten), und Versuchen in Schweden, dem Phänomen des *Downloading* und Schwarzbrennens von Alben und Filmen Herr zu werden. Als Gegenbewegung gründete sich dort am 1. Januar 2006 die weltweit erste Piratenpartei (Piratpartiet) (*Häusler* 2011, S. 19ff.; *Zolleis/Prokopf/ Strauch* 2010, S. 8ff.).

In der Uppsala-Erklärung, die 2009 auf der Konferenz der *Pirate Parties International* (PPI), einer Dachorganisation der nationalen Parteien, verabschiedet wurde, ging es u.a. um die Stärkung der Bürgerrechte durch Transparenz in der Regierungsarbeit und um das Recht auf anonyme Kommunikation auch auf digitalen Kanälen (Häusler 2011, S. 41ff.).

Im Grundsatzprogramm der deutschen Piraten heißt es: „Der Schutz der Privatsphäre und der Datenschutz gewährleisten Würde und Freiheit des Menschen." Die überwachte Gesellschaft entstehe allein schon dadurch, dass sie „technisch möglich" geworden sei und den Interessen von Wirtschaft und Staat gleichermaßen diene. Dieser Überwachung sage man entschieden den Kampf an. „Das Recht auf Wahrung der Privatsphäre ist ein unabdingbares Fundament einer demokratischen Gesellschaft." Jedem Bürger müsse das „Recht auf Anonymität" garantiert, das Briefgeheimnis solle zu einem generellen Kommunikationsgeheimnis erweitert werden. Der vorherrschende Kontrollwahn stelle eine weitaus ernsthaftere Bedrohung unserer Gesellschaft dar als der internationale Terrorismus (abgedruckt bei *Häusler* 2011, S. 147ff.).

Diese Position entspricht der sogenannten Hacker-Ethik mit ihrem Grundsatz: „Private Daten schützen, öffentliche Daten nützen" (*Heller* 2011, S. 111). Dieser Punkt wurde

in den achtziger Jahren vom Chaos Computer Club jenen Grundsätzen hinzugefügt, die schon länger in der Szene kursierten. Dabei ging es darum, den Schutz der Privatsphäre des Einzelnen mit dem freien Zugang von Informationen zu verknüpfen, welche die Allgemeinheit betreffen. Dieser Kodex bietet eine gewisse Orientierung, ist aber weder abschließend noch verbindlich.

In diesem Sinne weisen auch *Constanze Kurz* und *Frank Rieger* vom Chaos Computer Club darauf hin, „dass die lautesten Beschwörer des ‚Endes der Privatsphäre' die größten Profiteure dieser propagierten Entwicklung sind" (*Kurz/ Rieger* 2011, S. 9), und raten zur Vorsicht: „Sich der Bedeutung der Privatsphäre bewusst zu werden, darüber nachzudenken, wo die Grenzen sind, was man wirklich für sich behalten will, ist der erste Schritt zur digitalen Mündigkeit. Jeder von uns hat etwas zu verbergen – die Frage ist immer nur, vor wem" (ebenda, S. 11). Ihre Ratschläge – u.a. für jeden Service möglichst ein anderes Pseudonym zu verwenden (ebenda, S. 265; siehe auch *Kotteder* 2011) – dürften manchen Nutzer von Computer und Internet überfordern. Aber dass es der Schutz der Privatsphäre ist, der den Menschen vor dem Druck des Konformismus bewahrt, das habe der Jurist *Edward Bloustein* schon in den sechziger Jahren des vergangenen Jahrhunderts geschrieben (ebenda, S. 271).

Diese Position ist in der Netzgemeinde durchaus umstritten. Als *Constanze Kurz* diejenigen, die anderer Meinung sind, öffentlich als „Post-Privacy-Spackos" titulierte, nahmen diese den Fehdehandschuh gerne auf und kämpfen seither unter „Spackeria" gegen ein Festhalten an der Privatsphäre (www.spackeria.de). „Wir haben ja nichts dagegen, dass sich Leute im Netz nackig machen können", erklärte *Kurz*. „Man soll es nur nicht als Lebensstil, als soziale Norm propagieren." *Frank Rieger*: „Wir halten Post Privacy als Lebensstil für einen Irrweg", ein „ziemlich durchsichtiges Manöver von Google und Facebook" (zitiert bei: *Seeliger* 2010).

Für den Blogger *Christian Heller* hingegen ist die Privatsphäre ein Auslaufmodell: „Wir treten ein in das Zeitalter der ‚Post-Privacy': in ein Leben nach der Privatsphäre". Es lohne sich nicht, sie zu verteidigen, denn dieser Kampf sei längst verloren. Man könne ihn hier und da noch führen – aber nur aus taktischen Gründen und sicher nicht um jeden Preis. Das Ende der Privatsphäre bedeute nämlich nicht unbedingt den Weltuntergang. „Die Post-Privacy kommt – und wir sollten lernen, das Beste aus ihr zu machen" (*Heller* 2011, S. 7f.).

Laut dem amerikanischen Futuristen *David Brin* müssen wir unsere Freiheit anders verteidigen, als gegen die allgegenwärtige Überwachung anzukämpfen. Wenn wir gegenüber den Mächtigen schon keine Geheimnisse mehr bewahren könnten, dann sollten diese Daten wenigstens allen zur Verfügung stehen. Totale Überwachung werde dann zur totalen Transparenz. Darin hätten die Unteren weniger zu verlieren als die Oberen. In der Transparenten Gesellschaft, wie er sein Konzept nennt (*Brin* 1999), überwachen die Vielen das Oben, aber sich auch gegenseitig nach links und rechts. Das schwäche die Privatsphäre ebenso wie das Gewaltmonopol (zitiert bei: *Heller* 2011, S. 112f.). Wenn alles offen liege, wenn niemand mehr etwas zu verbergen habe, dann könne auch keiner mehr die Schwächen anderer ausnutzen. Die totale Demokratisierung der Überwachung mache Privatsphäre untereinander unmöglich.

Dass totale Transparenz ein erstrebenswertes Gesellschaftsmodell ist, ist zumindest strittig. Selbst wenn man das bejahen würde, bliebe immer noch die Frage, wie der Weg dahin aussehen könnte. Es ist ja nicht so, dass man von heute auf morgen bei Bürgern, Unternehmen und Staat – und zwar weltweit – einfach auf totale Transparenz umschalten könnte. Wenn aber einzelne Menschen, Unternehmen oder Staaten bereits „gläsern" sind,

während andere noch ihre Privatsphäre und ihre Geheimnisse schützen, dann machen sich jene sehr verletzlich und angreifbar. Gewalt, Macht und Interessen schmelzen auf dem Weg zu totaler Transparenz nicht einfach dahin (*Schmidt* 2012, S. 8). Intoleranz und Repression gegenüber Menschen, Diskriminierung und Skandalisierung von bestimmten Verhaltensweisen sind jedenfalls nicht ausgeschlossen, nur weil einige für eine offenere und tolerantere Welt kämpfen. Und wer nicht über entsprechenden Speicherplatz und hinreichende Rechenzeit verfügt, der könnte die schiere Menge der Daten bei totaler Transparenz weder auswerten noch sinnvoll nutzen.

Zuvor noch stellt sich die Frage, wer eigentlich darüber entscheidet, dass es künftig keinerlei Privatsphäre mehr geben soll. Mark Zuckerberg? Die „Spackeria"? Technische Sachzwänge? Oder demokratische Mehrheiten? Wer bestimmte Entwicklungen, die durch das Internet möglich geworden sind, als unabweisbar darstellt, versucht sich im Grunde einer öffentlichen Diskussion und demokratischer Entscheidung zu entziehen. Insofern steckt in Postulaten wie „Ende der Privatheit" und „totale Transparenz" ein Stück totalitäres Denken.

Am Rande: Der Schutz der Privatsphäre gehört zu den allgemeinen, unveräußerlichen Menschenrechten. Er findet sich nicht nur in Artikel 12 der Allgemeinen Erklärung der Menschenrechte vom 10. Dezember 1948, die inzwischen von den meisten Staaten unterzeichnet worden ist, sondern auch in Artikel 17 des Internationalen Paktes über bürgerliche und politische Rechte, dem sogenannten Zivilpakt, vom 19. Dezember 1966: „Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre oder seines Rufes ausgesetzt werden." Und: „Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen" (zitiert nach: *Bundeszentrale* 1999, S. 78).

Dass keineswegs alle Hacker private Daten respektieren, zeigte die Veröffentlichung der Namensliste der Unterstützer des Aufrufs „Wir sind die Urheber!" samt Adressen, Geburtsdaten und Telefonnummern im Netz. Ihre *Homepages* wurden durch gezielte Angriffe lahmgelegt. Es ging nicht um das bessere Argument, sondern Menschen, die eine andere Auffassung haben, sollten mundtot gemacht werden. Und das auch noch anonym. Eine bemerkenswerte Intoleranz gegenüber Andersdenkenden – und kein schöner Ausblick auf die Gesellschaft, die da auf uns zukommen soll.

Das von *Google* finanzierte „Co:llaboratory Internet & Gesellschaft" stellt zu Recht fest, „dass politische Entscheidungen zu Privatheit und Öffentlichkeit auf fundamental unterschiedliche Gesellschaftsmodelle hinauslaufen" (2011, S. 12). Klar sei jedenfalls, dass Privatheit (Verschlossenheit) und Öffentlichkeit (Transparenz) neuer Regelungen und Einstellungen bedürften. Entscheidende Stellschraube aller Zukunftsszenarien sei die Kontrollierbarkeit des Informationsflusses (ebenda, S. 58f.). Klar sei auch: „Wenn jede Information überall ist, gibt es keine Privatheit mehr" (ebd., S. 55). Die Vorstellung einer Intimsphäre bzw. Privatsphäre sei nicht nur „wissenschaftlich überholt", sondern werde auch „durch das Internet für jedermann sichtbar in Frage gestellt". Wir hätten zwar eine personale Identität, würden uns aber in verschiedenen sozialen Strukturen mit verschiedenen *Personas* (früher hätte man Rollen gesagt) bewegen. Diese Vielfalt lasse sich weder technisch modellieren noch von einem normalen Benutzer beherrschen. Insofern sei ein solches Konzept nicht praktikabel (ebenda, S. 27). So einfach ist das.

Was totale Transparenz künftig bedeuten könnte, zeigt ein Strategiepapier „Das Beschäftigungsmodell der Zukunft" des Software-Konzerns IBM (*Dettmer/Dohmen* 2012, S. 62ff.): Künftig soll nur noch eine kleine Kernbelegschaft, die für strategische Fragen

und das Management des Unternehmens zuständig ist, eine feste Anstellung bekommen. Für Projekte und für Dienste am Kunden hingegen sollen – je nach Bedarf – für einige Tage, Wochen, Monate oder Jahre jeweils irgendwo auf der Welt Mitarbeiter angeheuert werden, die ihre Arbeitskraft auf einer Internetplattform nach dem Vorbild von *Ebay* anbieten können. Die Menschen, die auf die Plattform gelassen werden, würden nach einem „Zertifizierungsmodell" (Blau, Silber oder Gold) – je nach Qualifizierung und Befähigung – gekennzeichnet, aber auch nach ihrer „digitalen Reputation" bewertet, nämlich ihren bisherigen Leistungen, pünktlichem Erscheinen, Termintreue, fristgerechten Abrechnungen, aber auch sozialem Engagement. Das berufliche Profil würde sich mit den Bewertungen bisheriger Auftraggeber und früherer Kollegen zu einer Art elektronischem Lebenslauf verdichten, der von Firmen aus aller Welt auf der Plattform eingesehen werden kann. Über „virtuelle Kioske" sollen sie Zugriff auf das Personal erhalten und entscheiden können, wen sie anheuern wollen und wen nicht.

Nationales Arbeitsrecht, bestehende Tarifverträge und verbindliche Lohnregelungen spielen dann keine Rolle mehr. Schon jetzt halten viele Konzerne rund zwanzig Prozent ihrer Belegschaft durch Zeitarbeit, Werkverträge, Befristung oder *Outsourcing* flexibel. Die Zahl der unbefristeten Vollzeitstellen ist von 1999 auf 2009 um 18,5 Prozent gesunken. Nur noch etwa die Hälfte aller Arbeitnehmer hat eine feste Stelle, zugleich sind atypische Erwerbsformen wie Leiharbeit um fast 79 Prozent angestiegen (*Dettmer/Dohmen* 2012, S. 63). Dass manche, die sich als „digitale Bohéme" betrachten, das „Leben jenseits der Festanstellung" sogar noch glorifizieren (*Friebe/Lobo* 2006), sei hier nur am Rande erwähnt.

Wer sich den Spielregeln des neuen Modells unterwirft, ist lückenlos transparent. Wer sich verweigert, kommt nicht auf die Bewerberliste („Talent Cloud"). Wessen „digitale Reputation" nicht die Beste ist, hat – weltweit – kaum eine Chance, erwählt zu werden. Dass jemand eine Zeit lang nicht perfekt funktioniert hat, weil es in der Ehe kriselte oder aus anderen Gründen, kann leicht zum Verhängnis werden: Was im elektronischen Werdegang steht, wird niemals vergessen. Keine Geheimnisse mehr, keine Privatheit mehr – eine „schöne neue Welt" (*Aldous Huxley*).

3. Auf dem Weg zum gläsernen Staat?

Die Piraten setzen sich zwar für ein Recht zur Wahrung der Privatsphäre ein, plädieren beim Staat aber für völlige Transparenz. Der Einblick in die Arbeit von Verwaltung und Politik auf allen Ebenen der staatlichen Ordnung sei ein fundamentales Bürgerrecht, heißt es im Grundsatzprogramm. Man müsse vom „Prinzip der Geheimhaltung" zu einem „Prinzip der Öffentlichkeit" kommen. Zur „Transparenz aller staatlichen Prozesse" gehöre unter anderem, dass ein jeder „effizient, komfortabel und mit niedrigen Kosten" Zugang zu staatlichen Informationen bekommen müsse und dass ein jeder unabhängig von persönlicher Betroffenheit und ohne irgendwelche Begründungen überall „Einsicht in die Aktenvorgänge" nehmen könne. Gewisse Schranken finde dieses Recht im Schutz von Persönlichkeitsrechten, in der nationalen Sicherheit, zur Verhinderung von Straftaten und ähnlichem. Diese Ausnahmen seien aber „möglichst eng und eindeutig" zu formulieren, damit nicht ganze Behörden oder Verwaltungsbereiche ausgeklammert werden könnten. Gemäß dem Recht auf Anonymität, das sie für die Bürger fordern, setzen sich die Piraten bei der von ihnen geforderten „Kennzeichnungspflicht für Polizeibeamte" immerhin dafür

ein, dass diese pseudonym (z.B. in Form einer Nummer) gestaltet werden darf (zitiert wiederum bei *Häusler* 2011, S. 151ff.).

Dass jeder einfach in alle Akten aller Behörden gucken darf, entspricht nicht der deutschen Verwaltungstradition. Dort, wo Anträge bearbeitet werden, handelt es sich immer um personenbezogene Daten. Aber auch in den meisten anderen Akten dürfte es Verweise auf handelnde Personen geben. Die Verwaltung ist in ihrem Handeln an Recht und Gesetz und an die Programme gebunden, die das Parlament beschließt. Sie soll diese Vorgaben ohne Ansehen der Person umsetzen, also „neutral", gerade ohne irgendwelche Einflüsterungen von Nachbarn, Lobbyisten oder Verbänden. Wenn die Mitarbeiter in den Behörden damit rechnen müssten, dass jeder ihrer Vermerke – auch die fachliche und/oder politische Bewertung von Eingaben – von jedermann gelesen werden kann, dann würde sich die Verwaltungspraxis radikal verändern.

Die Position der Piraten entspricht der alten Hacker-Ethik: „Private Daten schützen, öffentliche Daten nützen." Wenn aber nichts mehr behördenintern bleibt, müss(t)en die Mitarbeiter sich überlegen, was man überhaupt noch aufschreibt und zu den Akten gibt. Lobbyisten dürften sich freuen, lesen zu können, was in der Verwaltung über ihre Vorstöße gedacht wird, während ihre eigenen Planungen geheim bleiben. Opposition und Medien könnten jederzeit mitlesen, wie Regierung und Verwaltung sich positionieren. Ein „gläserner Staat" würde letztlich keine vertraulichen Informationen mehr bekommen.

Unsere alte Welt kannte (und kennt) aus guten Gründen eine ganze Reihe von Geheimnissen. Nicht nur Staatsgeheimnisse, Betriebs- und Geschäftsgeheimnisse, sondern auch das Bankgeheimnis und das Beichtgeheimnis, das Arztgeheimnis und das Anwaltsgeheimnis, das Steuergeheimnis und das Sozialgeheimnis – um nur einige zu nennen. Wir kennen nicht nur das Amtsgeheimnis und das Meldegeheimnis (§ 5 MRRG), sondern auch das Briefgeheimnis und das Fernmeldegeheimnis. Wenn jeder in alle Akten von Behörden gucken dürfte, dann gäbe es viele dieser Geheimnisse faktisch nicht mehr.

Menschen, die durch ihren Beruf ein Wissen über andere Menschen erwerben, das diese keinem Dritten anvertrauen würden, wenn sie nicht sicher sein könnten, dass es dann immer noch geheim bleibt, haben nicht nur das Recht, vor Polizei und Justiz das Zeugnis zu verweigern (§§ 53, 53a StPO, §§ 383 f. ZPO), sondern geradezu die Pflicht, dieses Wissen zu bewahren. Wer sich nicht daran hält, muss mit strafrechtlichen Sanktionen (§ 203 StGB) und auch mit standesrechtlichen Disziplinarmaßnahmen rechnen (*Heckmann/Seidl/Maisch* 2012).

Das Seelsorge- oder Beichtgeheimnis basiert eigentlich auf dem Kirchenrecht, ist aber staatlich anerkannt. Danach haben auch Geistliche das Recht und die Pflicht, das Zeugnis über das, was ihnen unter dem Siegel der Verschwiegenheit anvertraut worden ist, zu verweigern (§ 53 Abs. 1 Satz 1 Nr. 1 StPO). Ähnliches gilt für Journalisten.

Auch Ärzte – ob in öffentlichen Krankenhäusern oder mit privater Praxis – sind verpflichtet, über all das, was ihnen ein Patient anvertraut, zu schweigen. In ihrer Praxis müssen die Rechner so eingestellt sein, dass niemand zufällig Daten von Patienten auf dem Bildschirm einsehen kann. Für Banken sind Abstände zwischen den Beratungszonen vorgeschrieben, damit niemand etwas über die finanziellen Verhältnisse eines anderen hören kann. Eine ärztliche Schweigepflicht wird sogar schon für den bloßen Namen des Patienten angenommen sowie für die Tatsache, dass jemand überhaupt einen Arzt konsultiert hat.

Sinn und Zweck beruflicher Schweigepflichten ist es, eine Vertrauensbasis zwischen Arzt und Patient, zwischen Anwalt und Mandant und zwischen jenen, die sozialer Unterstützung bedürfen, und denen, die das zu prüfen und zu bewilligen haben, zu schaffen.

Wer wäre schon bereit, seine finanziellen Verhältnisse lückenlos zu offenbaren und über Möglichkeiten, eventuell Steuern zu sparen, bereitwillig zu diskutieren, wenn er nicht sicher sein könnte, dass der Steuerberater dichthält? Während man in anderen Ländern die Steuererklärungen von anderen problemlos einsehen kann, ist das Steuergeheimnis in Deutschland besonders geschützt (§ 30 AO). Es bindet nicht nur die Steuerberater und ihre Gehilfen, sondern auch die Finanzbehörden. Das ist der Grund, warum diese auf eigenen Rechenzentren innerhalb der Verwaltung bestehen und elektronische Steuerbescheide besonders verschlüsselt sein müssen (§ 87 Abs. 1 Satz 3 AO).

Ein Verteidiger, der erfolgreich sein will, muss wissen, was sein Mandant tatsächlich angestellt hat. Nur dann kann er eine Strategie wählen, die nicht durch überraschende Vorhaltungen des Staatsanwalts obsolet werden kann. Ein Straftäter wird aber nur erzählen, was er wirklich angestellt hat, wenn er sicher sein kann, dass der Anwalt das für sich behält. Die anwaltliche Schweigepflicht schützt nicht nur den Einzelnen, sie liegt – so schwer dies bei einzelnen Fällen nachvollziehbar erscheinen mag – in unser aller Interesse, da nur so eine funktionierende Rechtsordnung zustande kommen kann. Anwälte können ihre Mandanten nicht richtig beraten, wenn sie nicht wissen, was wirklich passiert ist. Und diejenigen, die etwas angestellt haben, werden alles leugnen, wenn sie nicht sicher sein können, dass der Anwalt mit vertraulichen Eingeständnissen professionell umgeht.

Wenn wir mit anderen Menschen nicht unter vier Augen, sondern über größere Strecken kommunizieren wollen, dann unterliegt auch diese Kommunikation – ob mit dem Anwalt oder mit der Freundin – dem Geheimnisschutz (Art. 10 GG). Das Briefgeheimnis schützt den Inhalt von Briefen, die wir verschicken, das Postgeheimnis schützt den Inhalt von Paketen und sonstigen Sendungen, die von Postdienstleistern befördert werden, und das Fernmeldegeheimnis schützt unsere Telefonate und unseren Mail-Verkehr. Es schützt „alle technisch verfügbaren Mittel der unkörperlichen Kommunikation“ (*Heckmann/Seidl/Maisch* 2012, S. 17).

Jedenfalls ist nicht nur das Abhören, das Aufzeichnen und die Kenntnisnahme des Inhalts geschützt, sondern auch die Erfassung der näheren Umstände, also die Erhebung von Verkehrsdaten wie beispielsweise Informationen über Zeit, Ort und die Art und Weise der elektronischen Kommunikation (*Schaar* 2009).

Diejenigen, die das Ende aller (staatlichen) Geheimnisse propagieren, sind der Auffassung, diese Schweigepflichten und Schutzrechte brächten letztlich nichts, da staatliche Behörden im Zweifel auch auf vertrauliche Kommunikation zugreifen könnten. Man wähnt sich ohnehin in einem Zeitalter totaler Überwachung (*Zeh/Trojanow* 2009; *Simon/Simon* 2008).

Richtig ist, dass der Staat unter bestimmten Umständen in Briefe und Pakete Einblick nehmen und auch Telefonate und Mailverkehre überwachen kann. Dieses Recht dient der Aufklärung von schweren Straftaten und unser aller Sicherheit. Um es ausüben zu können, bedarf es in jedem Einzelfall einer richterlichen Genehmigung. Es ist also nicht so, dass der Staat wahllos einen jeden abhören und überwachen darf. Dann hätten wir in der Tat den „gläsernen Bürger“ ohne jegliche Geheimnisse. Dass es trotz aller Technik und gewaltiger Datenspeicher faktisch nicht möglich ist, selbst wenn das rechtlich zulässig sein sollte, eine große Anzahl Menschen zu überwachen, weil alle Informationen lückenlos dokumentiert und gerichtsfest aufbereitet werden müssen, steht auf einem anderen Blatt.

Daniel Domscheit-Berg, Mitbegründer von *WikiLeaks*, aber dann im Streit mit *Julian Assange* geschieden (*Domscheit-Berg* 2011a) und jetzt auf dem Weg, eine ähnliche Platt-

form („*OpenLeaks*“) aufzubauen, sieht in dem Recht auf Geheimnisse, „vor allem für Individuen“, das Merkmal einer freien Gesellschaft. „Der Verrat von privaten Geheimnissen ist eine Verletzung.“ Und: „Der Schutz dieser Geheimnisse ist höchstes Gut einer freiheitlichen Gesellschaft. Ihre Wahrung und auch Achtung sind Aufgabe und Pflicht eines jedes (sic!) Einzelnen“ (*Domscheit-Berg* 2011b, S. 99).

Ihnen gegenüber stünden aber die „Geheimnisse von Firmen, Militärs und Regierungen, eben nicht von Individuen, sondern von Organisationen, von Systemen innerhalb unserer Gesellschaft.“ Diese würden Macht konzentrieren und ausüben. Deshalb müsse man sie anders betrachten. Wenn man sie kontrollieren wolle, brauche man Transparenz, „also das Gegenteil von Geheimhaltung“ (*Domscheit-Berg* 2011b, S. 99f.). „Transparenz, eine unabhängige Kontrolle und resultierend die Fähigkeit zur Korrektur von Fehlern sind missionskritisch, denn alles andere führt zur schleichenden Korruption der gesellschaftlichen Subsysteme – und als Folge daraus der Gesellschaft als Ganzes“ (ebenda, S. 102).

Dass sämtliche Staatsgeheimnisse, also Informationen, die vertraulich sind, zwingend zu Amtsmissbrauch und Korruption führen, ist ein Köhlerglaube. Korruption wird bekanntlich allgemein verstanden als „*misuse of public power for private profit*“ (*Joseph A. Senturia*). Viele Informationen würden staatliche Stellen gar nicht bekommen, wenn die Informanten nicht sicher sein könnten, dass sie vertraulich behandelt werden. Offenheit ist die Schwester der Vertraulichkeit. Mit Korruption hat das nichts zu tun. Manchmal geht es in der Politik nur um das richtige *Timing*, mit einer Information auf den Markt zu gehen. Wer den falschen Zeitpunkt wählt oder mit einem Vorschlag aufwartet, der nicht zu Ende gedacht oder noch nicht abgestimmt ist, hat häufig schon verloren.

Domscheit-Berg sieht das anders: „Da eine Zunahme von Macht in der Regel mit einer Zunahme des Missbrauchs von Geheimnissen einhergeht, wird der Geheimnisverrat zur Notwendigkeit, diesem Missbrauch entgegenzuwirken, als ein Mechanismus der Checks and Balances von unten.“ In diesem Sinne unterscheidet er zwischen „schlechtem“ Geheimnisverrat und „gutem“ Geheimnisverrat (*Domscheit-Berg* 2011b, S. 103).

Was „gute“ und was „schlechte“ Geheimnisse sind, soll nicht demokratisch entschieden, gesetzlich geregelt oder an klaren Kriterien orientiert, sondern offenbar jedem selbst überlassen werden. „Das Recht auf Geheimnisverrat ist ebenso wichtig wie das Recht auf Geheimnisse an sich. Viel spezifischer kann man es nicht sagen, alles Weitere wird wohl immer eine Einzelfallentscheidung sein“ (*Domscheit-Berg* 2011b, S. 103). Der Einzelne soll sich also über die Regeln, die für alle gelten, nach eigenem Gusto hinwegsetzen dürfen. Das ist nicht Demokratie, sondern Anarchie. Der Einzelne trägt damit, wenn er sich nicht auf Recht und Gesetz berufen kann, auch das volle Risiko (*Király* 2010, S. 29ff.). Immerhin plädiert *Domscheit-Berg* für „stärkere Gesetze“, „um jene Geheimnisverräter, die Whistleblower, vor Repressalien zu schützen“ (*Domscheit-Berg* 2011b, S. 103).

Ein „Recht auf Geheimnisverrat“ gibt es im Übrigen nicht. Beamte können, wenn sie der Ansicht sein sollten, ihre Führung mache etwas Illegales oder Illegitimes, dagegen *remonstrieren* und sie sind in bestimmten Fällen sogar verpflichtet, Meldung zu machen. Das ist der zentrale Grund dafür, warum es den Status eines Beamten, der unkündbar ist, überhaupt gibt. Das Restrisiko, womöglich versetzt oder nicht befördert zu werden, muss man in Kauf nehmen, wenn es um einen echten Skandal geht. Für die Meldung gibt es allerdings vorgeschriebene Wege innerhalb der Verwaltung, da sich nicht jeder Vorwurf oder Verdacht als berechtigt herausstellt (*Király* 2010). Der Dienstweg soll nicht der Vertuschung dienen, sondern der Behörde die Chance geben, Vorwürfe aufzuklären und ggfs. zur Anzeige zu bringen. Öffentliche Vorverurteilungen bleiben haften, auch wenn sie sich später als

falsch herausstellen. Staat und Verwaltung haben auch eine Fürsorgepflicht gegenüber Amtsträgern.

Mitarbeiter von Unternehmen, die Skrupel haben, dass alles legal oder legitim ist, was man treibt, und das öffentlich machen, müssen mit fristloser Kündigung rechnen. Sie müssen also abwägen, ob etwas so gravierend ist, dass man es öffentlich machen muss und dafür notfalls die Entlassung riskiert. Nicht jeder *Whistleblower* handelt übrigens selbstlos. Wer Bankdaten von Steuersündern verrät, möchte manchmal einfach nur ausgesorgt haben und nicht mehr arbeiten müssen.

Nicht jede Verschlusssache, die in Geheimschutzstellen lagert, müsste dort unbedingt liegen. Insofern ist die Diskussion darüber legitim, wie offen der Staat sein soll oder wie verschwiegen er sein darf. Die Informationsfreiheitsgesetze des Bundes und der Länder haben für die Bürgerinnen und Bürger neue Rechte gebracht, in die Verwaltungen hineinzusehen. Dass diese Rechte kaum genutzt werden – wie schon früher längst nicht alle öffentlichen Quellen ausgeschöpft wurden – und auch die vielen Datensätze und Dokumente, die inzwischen ins Netz gestellt werden, nur begrenzt Interesse finden, mag in der Natur der Sache liegen. Vieles von dem, mit dem sich Verwaltung zu beschäftigen hat, ist so spannend nicht. Das muss aber nicht daran hindern, noch mehr Offenheit von Staat und Verwaltung zu fordern (siehe etwa die „Bremer Erklärung").

Die Forderung nach noch mehr Offenheit von Staat und Verwaltung unterscheidet sich allerdings grundsätzlich von einem individuellen „Recht auf Geheimnisverrat", das jeder einfach für sich in Anspruch nehmen kann, wenn ihm danach ist. Dieses Plädoyer für Indiskretionen, Illoyalität und Verrat kann nur gutheißen, wer Verschwiegenheit, Loyalität und Geheimnisse für völlig überflüssig hält. Das wiederum würde nicht nur den Staat, sondern unsere ganze Gesellschaft radikal verändern. Gilt dieses Recht auch für Mitglieder von *Anonymus* oder für Mitarbeiter von *OpenLeaks* oder von *Facebook, Google & Co.*? Dass diese Gruppierungen und auch die Unternehmen Macht ausüben, dürfte außer Frage stehen (siehe die Beispiele bei *Reissmann/Stöcker/Lischka* 2012). Wie will *Apple* mit neuen Produkten noch Staunen hervorrufen, wenn alle längst wissen, was da kommt? Verrät in Zukunft also jeder jeden? Keine schöne neue Welt.

4. Eine zweifache Schwächung des demokratischen Staates

Dass Privates auch privat bleiben sollte, das war in der deutschen Gesellschaft nach 1945 Konsens. Über die eigene finanzielle Situation, über Krankheiten und Beziehungssorgen redete man nicht – nicht einmal mit Freunden oder Nachbarn und schon gar nicht mit Fremden oder Journalisten (*Scherz/Höch* 2011, S. 17f.).

Während früher Telefonzellen gelb waren und schalldicht isoliert, damit niemand draußen das Gespräch mithören konnte, bekommen wir heute überall ungewollt mit, was andere am Handy erzählen. Menschen entblößen sich im Fernsehen in einer Weise, die früher als peinlich gegolten hätte und versteckt worden wäre. Das Internet bzw. das interaktive Web 2.0, in dem jeder selbst Inhalte einstellen kann, ohne dass es professionelle Filterinstanzen gäbe, verstärkt diesen Trend zur öffentlichen Selbstdarstellung. „Der Insasse des digitalen Panoptikums ist Opfer und Täter zugleich" (*Han* 2012b, S. 82).

Zum Konsens, den wir früher hatten, gehörte auch, dass es neben privaten Geheimnissen auch staatliche Geheimnisse gibt: Geheimdiplomatie, vertrauliche *backchannels* zwischen West und Ost, diskrete Sondierungen zwischen konkurrierenden Parteien oder ver-

feindeten Nationen (wie Israelis und Palästinensern), das Arkanum der Kabinette. Dass Regierungen eine geschützte Sphäre brauchen, in der sie offen strategische und taktische Fragen abwägen können, hat das Bundesverfassungsgericht mehrfach anerkannt. Auch zum Amtsgeheimnis und zum Geheimnisverrat gibt es eine gesicherte Rechtsprechung.

Man mag, wie gesagt, darüber streiten, ob alles, was als Verschlusssache („VS – Nur für den Dienstgebrauch") in Geheimschutzstellen abgeheftet ist, wirklich so bedeutsam ist, dass es dort lagern muss. Aber dass man, wenn man Politik machen will, nicht immer offen über alles reden kann, was man weiß oder erfährt, war jedenfalls bisher nicht strittig. Ohne Vertraulichkeit zu garantieren, würde man manche Informationen gar nicht erst bekommen. Das gilt keineswegs nur für Nachrichtendienste. Insofern ist gegen eine Diskussion darüber, ob *mehr* Transparenz möglich und sinnvoll ist, überhaupt nichts einzuwenden, wohl aber gegen Forderungen nach *totaler* Transparenz. Denn diese Forderung entspringt totalitärem Denken. Schon bei Rousseau lasse sich beobachten, schreibt *Byung-Chul Han*, „dass die Moral totaler Transparenz notwendig in Tyrannei umschlägt" (*Han* 2012b, S. 72). Am Ende stehe eine inhumane Kontrollgesellschaft.

Die Verfechter einer totalen Transparenz argumentieren hingegen, nur so ließen sich Machtmissbrauch und Korruption eindämmen. Dass keine Organisation erfolgreich sein kann, die von vornherein alles öffentlich verhandelt, und dass es durchaus sinnvoll sein kann, Papiere vertraulich zu behandeln, bis sie einen gewissen Reifegrad erreicht haben, das verstehen sie nicht. Mit Korruption und Missbrauch hat das alles nichts zu tun, sondern lediglich mit notwendigen Spielregeln und bewährten Verfahren. Dass gerade jene, die von anderen totale Transparenz einfordern, sich wie Sekten oder Geheimdienste verhalten, wenn es um Informationen über handelnde Personen und die Organisation und ihre Pläne handelt, gehört zur Ironie der Geschichte.

Byong-Chul Han, der an der Hochschule für Gestaltung in Karlsruhe Philosophie lehrt, hat darauf hingewiesen, dass man die Tragweite von Transparenz verkenne, wenn man sie nur auf mehr Demokratie oder die Bekämpfung von Korruption reduziere. Transparenz manifestiere sich heute als „ein systemischer Zwang", der alle gesellschaftlichen, ökonomischen und politischen Prozesse erfasse und sie einer tief greifenden Veränderung unterwerfe. Die Transparenzgesellschaft sei eine Positivgesellschaft, wo sich alle Handlungen einem berechen-, steuer- und kontrollierbaren Prozess unterwerfen, eine „Hölle des Gleichen". Transparenz sei ein Instrument der Kontrolle und der Überwachung, ein „neues Wort für Gleichschaltung" (Ulrich Schacht) (*Han* 2012a, S. 41).

Das Bestreben, durch Transparenz Vertrauen zu schaffen, berge einen Widerspruch in sich. Denn Vertrauen sei nur möglich in einem Zustand zwischen Wissen und Unwissen. Wenn alles bekannt sei, erübrige sich Vertrauen: „Wo die Transparenz herrscht, ist kein Raum für das Vertrauen." Statt „Transparenz schafft Vertrauen" sollte es eigentlich heißen: „Transparenz schafft Vertrauen ab." In einer auf Vertrauen beruhenden Gesellschaft entstehe keine penetrante Forderung nach Transparenz. Die Transparenzgesellschaft sei eine „Gesellschaft des Misstrauens und des Verdachts, die aufgrund schwindenden Vertrauens auf Kontrolle setzt" (*Han* 2012b, S. 78f.).

Ein Mehr an Information bringe allein keine systemische Erneuerung oder Veränderung hervor. Die Ideologie der „Post Privacy", die im Namen der Transparenz eine totale Preisgabe der Privatsphäre fordere, sei nicht minder naiv: „Der Mensch ist nicht einmal sich selbst transparent." Gerade die fehlende Transparenz des anderen erhalte eine Beziehung lebendig. *Han* zitiert *Georg Simmel*: „Die bloße Tatsache des absoluten Kennens, des psychologischen Ausgeschöpfthabens ernüchtert uns auch ohne vorhergehenden Rausch, lähmt die

Lebendigkeit der Beziehungen. Die fruchtbare Tiefe der Beziehungen, die hinter jedem geoffenbarten Letzten noch ein Allerletztes ahnt und ehrt, ist nur der Lohn jener Zartheit und Selbstbeherrschung, die auch in dem engsten, den ganzen Menschen umfassenden Verhältnis noch das innere Privateigentum respektiert, die das Recht auf Frage durch das Recht auf Geheimnis begrenzen lässt." Die menschliche Seele brauche offenbar Sphären, wo sie bei sich sein könne, ohne die Sorge um den Blick des anderen: „Eine totale Ausleuchtung würde sie ausbrennen", totale Transparenz womöglich zu einer Art *Burn-out* der Seele führen. Ganz transparent sei nur die Maschine. Eine transparente Beziehung sei eine tote Relation, der jede Anziehung fehle: „Transparent ist nur das Tote" (*Han* 2012a, S. 41).

Han hat nichts gegen die Verteidigung der Menschenrechte oder die Bekämpfung der Korruption. Seine Kritik gilt der Ideologisierung, Fetischisierung und Totalisierung von Transparenz. Ihn treibt die Sorge um, „dass die Transparenzgesellschaft heute in eine Kontrollgesellschaft umzuschlagen droht" (*Han* 2012a, S. 41).

Der Hinweis von *Niklas Luhmann*, dass man Kontrolle – aus zeitlichen und aus fachlichen Gründen – ernsthaft „nur im Hauptberuf" ausüben könne (*Luhmann* 2009, S. 77), scheint bei den Verfechtern totaler Transparenz und Kontrolle noch nicht angekommen sein. Der normale Bürger, der seine Familie ernähren muss und noch andere Interessen hat, wäre mit einer lückenlosen Überwachung von Politik und Staat überfordert. Er überlässt diese Aufgabe der Opposition und den Medien, den Rechnungshöfen und Gerichten – und zieht daraus bei der nächsten Wahl seine Schlüsse.

Der Zwang zur Transparenz sei letzten Endes, so *Han*, kein ethischer oder politischer, sondern ein ökonomischer Imperativ: „Ausleuchtung ist Ausbeutung." Der transparente Kunde sei der neue Insasse, ja der neue Homo sacer des ökonomischen Panoptikums. Die Besonderheit des digitalen Panoptikums sei, dass seine Bewohner selbst an dessen Bau und an dessen Unterhaltung aktiv mitarbeiten, indem sie sich zur Schau stellen und entblößen. Deshalb vollziehe sich heute die Überwachung nicht als Angriff auf die Freiheit (*Zeh/Trojanow* 2009): „Vielmehr fallen Freiheit und Kontrolle in eins – wie auch der transparente User Opfer ist und Täter zugleich." Jeder baue fleißig mit am Panoptikum der Netze (*Han* 2012a, S. 41).

Nicht erst der Ruf nach totaler Transparenz und dem völligen Abbau staatlicher Geheimnisse und der beamtenrechtlichen Verschwiegenheitspflicht, sondern schon die Diskussion um „*Open Government*" und „*Open Data*" zielt auf eine weitere Machtverschiebung zwischen Staat und Wirtschaft. Dass die Nationalstaaten Mühe haben, ihrer Rolle gerecht zu werden, zeigen nicht nur die Turbulenzen auf den Finanzmärkten. Der „gläserne Staat" würde gegenüber einer Wirtschaft, die ihre eigenen Pläne und Strategien sorgsam geheim hält, noch weiter ins Hintertreffen geraten. Die ohnehin prekäre Balance zwischen Wirtschaft und Staat würde noch weiter aus dem Lot geraten.

In einer Demokratie haben die Bürger vielfältige Möglichkeiten, sich über staatliches Handeln zu informieren. Vieles, was früher nur als gedrucktes Papier zugänglich war, steht heute im Netz. Die Medien berichten ständig darüber, was innerhalb der Regierung gedacht wird; selbst Politiker *twittern* inzwischen. Wer noch mehr wissen will, kann sich auf die Informationsfreiheitsgesetze des Bundes und der Länder berufen. Staatliches Handeln ist – jedenfalls in Demokratien – heute transparenter denn je. Und darin läge eine zweite Schwächung durch totale Transparenz: Für Diktaturen gälte das nicht, sie würden sich weiter abschotten. In ihnen zählt das private Geheimnis nichts und das staatliche alles.

Ob man die doppelte Schwächung des demokratischen Staates durch totale Transparenz – gegenüber der Wirtschaft, gegenüber Diktaturen – für sinnvoll hält oder nicht,

muss letztlich jeder für sich selbst entscheiden. In Demokratien darf man das bekanntlich, auch wenn manche Verfechter totaler Transparenz und des „Endes der Privatsphäre" mit demokratischen Spielregeln eher auf Kriegsfuß zu stehen scheinen. Ihnen möchte man mit *Byung-Chul Han* zurufen: „Mehr an Information und Kommunikation allein *erhellt* die Welt nicht. Die Durchsichtigkeit macht auch nicht hellsichtig" (*Han* 2012b, S. 68).

Die Piraten nehmen in diesen Debatten eine mittlere Position ein. Sie verteidigen – auch nach der Erweiterung ihres Grundsatzprogramms vom 3./4. Dezember 2011 durch das Kapitel „Freier Zugang zu öffentlichen Inhalten" und des Unterkapitels „Offene Verträge mit der Wirtschaft" – eindeutig die Privatsphäre des Menschen, wollen aber für den Staat eine nahezu totale Transparenz („Akteneinsicht für jedermann"). Und sie sehen im *Whistleblowing* eine Form der Zivilcourage, die unbedingt unterstützt und geschützt werden müsse. In diesem Sinne wenden sie sich gegen eine Einteilung in gute und schlechte *Whistleblower* und plädieren für einen „generellen und umfassenden Schutz für Whistleblower mit notwendigen Ausnahmen" – was immer das heißen mag.

Auf den entsprechenden Gesetzentwurf, der das nachvollziehbar und überzeugend zu regeln versucht, darf man gespannt sein. Die Ermutigung zu Indiskretion, Illoyalität und Verrat, die in diesem Denken steckt, und auch ein völlig gläserner Staat und eine völlig offene Verwaltung, wie sie den Piraten vorschweben, würden unsere Gesellschaft, so diese Forderungen Realität würden, massiv verändern. Es hat nicht den Eindruck, dass sie schon zu Ende bedacht haben, was das tatsächlich bedeuten würde. Der Schwarm ist also noch unterwegs.

Literatur

Barlow, John Perry, 1996: Unabhängigkeitserklärung des Cyberspace (www.heise.de/1/1028/1.html).

Bieber, Christoph, 2012: Die Piratenpartei als neue Akteurin im Parteiensystem, in: Aus Politik und Zeitgeschichte, 62. Jahrg., Heft 7, S. 27-33.

Boveri, Margret, 1976: Der Verrat im 20. Jahrhundert. Mit einem Geleitwort von Gustav Heinemann und einer Einführung von Hellmut Becker, Reinbek bei Hamburg: Rowohlt.

Brin, David, 1999: The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?, Reading/Mass: Perseus.

Bundeszentrale für politische Bildung (Hrsg.), 1999: Menschenrechte. Dokumente und Deklarationen, 3., aktualisierte und erweiterte Aufl., Bonn.

Dettmer, Markus/Dohmen, Frank, 2012: Frei schwebend in der Wolke, in: Der Spiegel vom 6. Februar, S. 62-64.

Domscheit-Berg, Daniel, 2011a: Inside WikiLeaks. Meine Zeit bei der gefährlichsten Website der Welt, Düsseldorf: Econ.

Domscheit-Berg, Daniel, 2011b: Geheimnisse und die Gesellschaft, in: *Kretschmer, Birte /Werner, Frederic* (Hrsg.), Die digitale Öffentlichkeit. Wie das Internet unsere Demokratie verändert, Hamburg (Broschüre), S. 99-105.

Executive Office of the President of the United States, 2012: Consumer Data Privacy in a networked World: A Framework for protecting Privacy and promoting Innovation in the global digital Economy, Washington.

Friebe, Holm/Lobo, Sascha, 2006: Wir nennen es Arbeit. Die digitale Bohème oder: Intelligentes Leben jenseits der Festanstellung, 3. Aufl., München: Heyne.

Geiselberger, Heinrich, 2011 (Red.): Wikileaks und die Folgen. Netz – Medien – Politik, Berlin: Suhrkamp.

Häusler, Martin, 2011: Die Piraten Partei. Freiheit, die wir meinen. Neue Gesichter für die Politik, Berlin/München: Scorpio.

Han, Byong-Chul, 2012a: Transparent ist nur das Tote, in: Die Zeit vom 12. Januar, S. 41.

Han, Byong-Chul, 2012b: Transparenzgesellschaft, Berlin: Matthes & Seitz.

Heckmann, Dirk/Seidl, Alexander/Maisch, Michael Marc, 2012: Adäquates Sicherheitsniveau bei der elektronischen Kommunikation. Einsatz des E-Postbriefs bei Berufsgeheimnisträgern, Stuttgart: Boorberg.
Heinrich-Böll-Stiftung (Hrsg.), 2011: #public_life. Digitale Intimität, die Privatsphäre und das Netz, Berlin (Broschüre).
Heller, Christian, 2011: Post-Privacy. Prima leben ohne Privatsphäre, München: C.H. Beck.
Hirscher, Gerhard, 2011: Die Wählerschaft der PIRATEN-Partei, München (Hanns-Seidel-Stiftung).
Humborg, Christian, o.J. (2011): Reflektion zu Transparenz und Politik (Forum Berlin der Friedrich-Ebert-Stiftung 04), Berlin (Broschüre).
Internet & Gesellschaft Co:llaboratory (Hrsg.), 2010: „Offene Staatskunst". Bessere Politik durch „Open Government"? Abschlussbericht, 2. Aufl., Berlin (Broschüre).
Internet & Gesellschaft Co:llaboratory (Hrsg.), 2011: „Gleichgewicht und Spannung zwischen digitaler Privatheit und Öffentlichkeit". Phänomene, Szenarien und Denkanstöße. Abschlussbericht, Berlin (Broschüre).
Khatchadourian, Raffi, 2011: Keine Geheimnisse – Julian Assanges Mission der totalen Transparenz. Porträt eines Getriebenen, in: *Geiselberger, Heinrich* (Hrsg.), WikiLeaks und die Folgen, S. 11-46.
Király, Andrei, 2010: Whistleblower in der öffentlichen Verwaltung. Ihre Rechtsstellung bei der Korruptionsbekämpfung, Speyer (FÖV Discussion Paper 57).
Kotteder, Franz, 2011: Die wissen alles über sie. Wie Staat und Wirtschaft ihre Daten ausspionieren – und wie Sie sich davor schützen, München: Redline Verlag.
Kurz, Constanze/Rieger, Frank, 2011: Die Datenfresser. Wie Internetfirmen und Staat sich unsere Daten einverleiben und wir die Kontrolle darüber zurückerlangen, Frankfurt a. M.: Fischer.
Luhmann, Niklas, 2009 (zuerst 1968): Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität, 4. Aufl., Stuttgart: Lucius & Lucius..
Reissmann, Ole/Stöcker, Christian/Lischka, Konrad, 2012: We are Anonymous. Die Maske des Protests: wer sie sind, was sie antreibt, was sie wollen, München: Goldmann.
Rosenbach, Marcel/Stark, Holger, 2011: Staatsfeind WikiLeaks. Wie eine Gruppe von Netzaktivisten die mächtigsten Nationen der Welt herausfordert, München: DVA.
Schaar, Peter, 2007: Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft, München: Bertelsmann.
Schertz, Christian/Höch, Dominik, 2011: Privat war gestern. Wie Medien und Internet unsere Werte zerstören, Berlin: Ullstein.
Schilbach, Friederike (Hrsg.), 2011: Die Piraten Partei. Alles klar zum Entern?, Berlin: Bloomsbury Verlag.
Schmidt, Jan-Hinrik, 2012: Das demokratische Netz?, in: Aus Politik und Zeitgeschichte, 62. Jahrg., Heft 7, S. 3-8.
Seeliger, Julia, 2010: Der Innenminister als Troll, in: Die Tageszeitung vom 29. Dezember.
Simon, Anne-Catherine/Simon, Thomas, 2008: Ausgespäht und abgespeichert. Warum uns die totale Kontrolle droht und was wir dagegen tun können, München: Herbig.
Stoye, Sabine, 2012: Politik aus Notwehr – die Piratenpartei im Aufwind. Personen, Positionen, Perspektiven, Berlin (Konrad-Adenauer-Stiftung).
Zeh, Julie/Trojanow, Ilija, 2009: Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte, München: Hanser.
Zolleis, Udo/Prokopf, Simon/Strauch, Fabian, 2010: Die Piratenpartei. Hype oder Herausforderung für die deutsche Parteienlandschaft?, München (Hanns-Seidel-Stiftung).

Anschrift des Autors:
Dr. Göttrik Wewer, Vice President E-Government, Deutsche Post Consult GmbH, Kurt-Schumacher-Straße 28, 53113 Bonn
E-Mail: goettrik.wewer@deutschepost.de,
E-Postbrief: goettrik.wewer@deutschepost.epost.de.