Dieter Klumpp

Aufhaltsamer Abstieg zur Heteronomie in einer Softwarewelt?

„Unter Vorbehalt unvorhergesehener Entwicklungen läßt sich also sagen", schrieb Wilhelm Steinmüller zehn Jahre nach dem „denkwürdigen Spruch des BVerfG vom 15. Dezember 1983, das versuchte, im letzten Augenblick dem ‚informationellen Selbstbestimmungsrecht' des Betroffenen gegenüber der Wucht der zweiten Industrialisierung wieder zu seinem Recht zu verhelfen" (Steinmüller 1993, 701), dass sich die materielle Rechtslage dramatisch verschlimmert habe. Es werde „seit 1986 zusammen mit bereits vorhandenen oder neu geschaffenen Polizei-, Geheimdienste- und Datengesetzen unter allzu souveränem ‚Umgang' mit den Zweckbindungskriterien des BVerfG eine *neuartige Organisationsform* der Verwaltung begründet, die man als ‚autoritäre Datendemokratie' bezeichnen könnte. Sie unterläuft die in Recht und Verfassung begründete (und juristisch weiterbestehende) ‚informationelle Gewaltenteilung' der Behörden durch umfassenden Einsatz modernster Informationstechnologie-Mittel auf neue Weise, indem der gesamte Sicherheitsapparat unter Einschluß der Geheimdienste und aller ihrer Informationssysteme zu einer informationellen Verbundeinheit zusammengefaßt und zugleich der öffentlichen Kontrolle entzogen wird. Dies kontrastiert eigenartig mit der demokratischen Staatsform im übrigen" (ebd., 703).

Steinmüllers „Vorbehalt unvorhergesehener Entwicklungen" bei dieser Vorhersage war dem damals noch weithin gültigen wissenschaftlichen Ethos geschuldet, der solche powerpointigen Apodiktionen grundsätzlich ausschloss. Aus heutiger Sicht liest sich die zitierte Passage geradezu wie eine Drehbuchvorlage für die in der Folge eingetretene Entwicklung, wenn man zum Beispiel die

Verblüffung des US-Präsidenten angesichts des bürokratischen Eigenlebens betrachtet. Unvorhersehbare Ereignisse wie der Terrorschock vom September 2001 und der von Edward Snowden im Juni 2013 am Beispiel der NSA-Überwachung für jedermann ausgelöste Datentransparenzschock haben daran nichts geändert.

Der darob erstaunte Stoßseufzer von – unrettbar im Geiste der Aufklärung und der Idee des demokratischen Rechtsstaats verankerten – Zeitgenossen „Stell dir vor, es gibt ein Grundrecht – und keiner nimmt es wahr" könnte nach über vierzig Jahren eine kritische Zwischenbilanz des Rechts auf informationelle Selbstbestimmung und dessen Enkulturationsstatus bei den „Beteiligten" (in der Terminologie Steinmüller 1993, 304) intonieren. Kein Zweifel: Dieses Grundrecht („bis heute das wichtigste Recht, wenn es um Fragen des Datenschutzes geht", vgl. Borchers 2013, 1) erscheint auf unabsehbare Zeit in Deutschland unerschütterlich, auch wenn es nicht ausformuliert im Grundgesetz steht. Es würde wohl sogar eine Volksabstimmung mit Höchstquote bestehen, gäbe es eine solche denn. Auch das informationsethische Fundament ist absolut erschütterungssicher, eine feste Verankerung bis hinein in die Allgemeine Erklärung der Menschenrechte ist gegeben (vgl. umfassend: Capurro 2014).

Für die unverzagte Minderheit eines „räsonierenden Publikums" beklagte Gerhart Baum schon 2009 „das fatale Desinteresse vieler Bürger an ihren Bürgerrechten" (Baum 2009, 9) und konnte mit dem Enzensberger-Diktum eines „postdemokratischen Zustands" nur feststellen, dass „die fundamentalen Auswirkungen der digitalen Revolution nicht zu einer Sensibilisierung und Mobilisierung der Menschen geführt haben" (Baum 2013, 2). Dennoch gilt es, vor dem Hintergrund der NSA-Spähaffäre in vollem Umfang die Einschätzung von Constanze Kurz, der Sprecherin des heute geradezu als gouvernementale Diskursinstanz einzuordnenden Chaos Computer Club hervorzuheben: „Dass sich diese Woche weltweit Schriftsteller und Kreative zusammengefunden haben, um ihrer Ohnmacht und

ihrem Wunsch nach Konsequenzen aus der globalen Überwachung Ausdruck zu verleihen, verursacht im politischen Raum kaum ein Achselzucken“ (Kurz 2013, 2). Man kann nur hinzufügen, dass dieses Gefühl der Ohnmacht samt einem Wunsch nach Konsequenzen zumindest alle Kundigen – von der Wissenschaft bis zur über- und außerparteilichen Politik sowie aller drei Staatsgewalten – erfasst.

Die informationelle Selbstbestimmung als vorbildgebendes Grundrecht mit klarer verfassungsrechtlicher Ausdeutungslinie steht unversehens auf einer Stufe mit den vielen unsäglichen Leerbegriffen (z. B. „Digitale Demokratie“, „Innovation 2.0“ oder „Open Data“), die mit gutem Klang mittelfristig bestenfalls als modische Überschriften taugen. Es ist für das von Steinmüller diagnostizierte „noch wenig erwachte Datenschutzbewusstsein (…) der Öffentlichkeit“ (Steinmüller 1993, 700) bezeichnend, dass es der 30. Jahrestag des „Volkszählungsurteils“ vom 15. Dezember 1983 nirgendwo auch nur zu einer kleinen Feierstunde brachte. Steinmüller hatte auch diese Entwicklung schon in einer Zwischenbilanz bitter prognostiziert: „Ein Grundrecht stellt keinen Wert an sich dar. Vielmehr ist zu fragen, ob *dieses* Recht mehr oder besseren Schutz gewährt als die Rechtslage vorher. Das ist keineswegs stets der Fall; die Bürokratie hat bisher immer versucht (und z. T. erreicht), durch geschickte Formulierungen faktische Verschlechterungen zu ihren Gunsten zu erlangen“ (Steinmüller 1993, 699 f.). Die Tendenz beim Datenschutz sei „zwar nicht kleinster gemeinsamer Nenner, aber doch Handelsschutz vor Datenschutz“ (ebenda).

Verwunderlich ist dabei im Rückblick zunächst nur, dass Deutschland dieses großartige Leitbild der informationellen Selbstbestimmung seit 1971 nicht in alle Welt zu exportieren vermochte (so schon früh die Frage von Bernd Lutterbeck), sondern sich in rhythmischen Intervallen vielerorts sogar ein Image als „übereifriger Datenschützer“ anhängen lassen musste, es sich dann und wann auch selbst bescheinigte. Hoffmann-Riems Feststellung mit Bezug auf das

Lüth-Urteil des Bundesverfassungsgerichts 1958, dass ein „Auftrag an den Staat, die allgemeine Rechtsordnung so einzurichten, dass Freiheitsschutz auch gegen Private möglich sein muss“ besteht, (Hoffmann-Riem 2011, 1) wird lediglich in selbstreferenziellen Äußerungen von Wirtschaftsverbänden zwar regelmäßig, aber noch folgenlos bezweifelt. Festzustellen ist: Wenn der Staat in seiner Finanzierungsverzweiflung hoheitliche Funktionen per Outsourcing an Private verschiebt, muss er logischerweise auch ein Stück staatlichen Gewaltmonopols mitliefern.

Es oszilliert ein Handlungsvollzug des Grundrechts ziellos zwischen poesis und praxis. Denn die Jugend – ach! – ist eine vernetzte. Bundespräsident Gauck konstatierte zum 3. Oktober 2013: „Vor 30 Jahren wehrten sich Bundesbürger noch leidenschaftlich gegen die Volkszählung und setzten am Ende das Recht auf informationelle Selbstbestimmung durch. Und heute? Heute tragen Menschen freiwillig oder gedankenlos bei jedem Klick im Netz Persönliches zu Markte, die Jüngeren unter uns vertrauen sozialen Netzwerken gleich ihr ganzes Leben an“ (Gauck 2013). Auch Hoffmann-Riem sieht dies ähnlich: „Die Facebook community scheut sich nicht, private, ja intime Daten weiterzugeben, über die meine Eltern nicht einmal mit rotem Kopf gesprochen hätten. Leichtfertiger Umgang mit privaten Daten ist aber keine Rechtfertigung für den Staat, auf solche Daten ungehemmt zuzugreifen“ (Hoffmann-Riem 2011, 2). Die angeblich unbedachte Netzjugend ist zwar sicherlich der dominierende Cantus Firmus der Kunst der Boulevard-Fuge, aber „gezwungenermaßen“ ist eben nicht gleichbedeutend mit „freiwillig“ und „unwissend“ ist eben nicht „gedankenlos“, wie zu zeigen sein wird. Fest steht (auf den Repräsentativitätszweifel sei hingewiesen): Bürger gehen für ein doch offensichtlich von 87 % der deutschen Bevölkerung unterstütztes Grundrecht auf informationelle Selbstbestimmung auch dann nicht auf die Straße, wenn man ihnen digitaldividenderisch versichert, dass sie dort für die Funksignale der

Smartphones immerhin bessere physikalische Bedingungen als im traut-vernetzten Heim haben.

Nutzergruppen: Freiwillige und Nicht-Freiwillige

Die Netznutzer (nach Steinmüller wären dies „alle Beteiligten, die Online eine Systemleistung erwarten oder verwerten") lassen sich in zwei Gruppen unterscheiden, die je für sich empirisch exakt schwer fassbar sind. Tatsächlich gibt es eine besonders tiefe digitale Spaltung zwischen Menschen einerseits, die zwar von erforderlicher „Datensparsamkeit" oder „Medienkompetenz" sprechen, aber im Grunde die Wahlmöglichkeit einer überwiegenden *Netzabstinenz* für sich selbst durchaus als noch gegeben erachten. Diese über alle Altersstufen reichende Gruppe vermag Heteronomien wie das Ausspähen der Privatheit durch unbekannte Dritte mit dem Hinweis auf die Freiwilligkeit zu akzeptieren, denn „man macht ja schließlich freiwillig mit", trivialiter: „alles Persönliche macht man eben nur persönlich". Die Attitüde eines Teils dieser Gruppe lässt sich zunächst auf die seit Jahren vor allem in den USA diskutierte allgemeine Reaktionsbewegung „We have nothing to hide" reduzieren, muss jedoch in Bezug auf ihre Granularität und Rückbezüglichkeit gerade in Deutschland noch deutlich hinterfragt werden.

Auf der anderen Seite steht eine wachsende Gruppe von vor allem jüngeren Menschen, die sich ihr privates und familiäres Beziehungsleben ohne „Internet" (empfunden jeweils als Online-Aggregatzustand von Google, Facebook, Twitter, Youtube, SMS oder Skype und dann und wann ein Festnetztelefon) gar nicht mehr vorstellen kann. Auch für das gesellschaftliche Medienerlebnis in der Peer Group oder am Arbeitsplatz braucht sie nur noch das entstandene Selbstbedienungs-Netz, nicht mehr die abonnierte Tageszeitung, schon gar nicht die Haushaltsabgabe des öffentlich-rechtlichen Rundfunks samt deren in der Internetgemeinde heftig kritisierten

„GEZ-Schnüfflern". Diese zweite Gruppe steht einer fremdbestimmten Interaktionsmöglichkeit (etwa schon der Ausspähpotentialität) zwar in jeder Hinsicht kritisch gegenüber, die Alternative, „ohne Netz zu leben" wäre für sie aber die größte anzunehmende soziale Heteronomie, trivialiter: „Nutzer kann man ja nur als Nutzer sein". Dies ist also keineswegs unbedacht, sondern durchaus im grundlegenden Axiom der Rationalität: „Menschen entscheiden sich für diejenigen Handlungen, deren Folgen sie gegenüber den Folgen jeder anderen realisierbaren Handlung bevorzugen" (Elster 1987, 22).

Beiden Gruppen ist zunächst gemeinsam, dass sie sich rational auf „instantane Akzeptanz" (Klumpp 2012, 128 f.) eingerichtet haben. Was praktisch ist, ist gut, wissen schon seit 1967 die Nutzer von Taschenrechnern, und wie bei „allen elektronischen Dingen" wird alles auch jedes Jahr billiger. Zur instantanen Akzeptanz des Internet gehört die Annahme, dass es sich um eine Modernisierung von Telefon und TV handelt, die beide enkulturiert als „sicher" gelten. Kein Wunder: Seit Beginn der Meinungs- und Delphi-Umfragen zum Internet steht der Begriff „Sicherheit" (im Deutschen ein gewohnt diskussionsverwirrender Sammelbegriff für so unterschiedliche Bedeutungen wie „Security, Safety, Robustness, Availability, u. v. a. m., vgl. unübertroffen: Müller/ Pfitzmann 1997) unangefochten immer mit Abstand an der Spitze, weshalb beide Gruppen bei einer Wichtigkeitsentscheidung mehrheitlich stets die „Sicherheit" vor alles andere stellen werden, selbst vor die „Freiheit", die im Deutschen ja ebenfalls eine höhere Mehrdeutigkeit impliziert, nämlich Freiheit *zu* allem Gewohnten bis hin zur Freiheit *von* Kosten. Die gespaltene Meinung der Nutzer wird nicht nur in Deutschland deutlich: Gemäß einer durchaus repräsentativen Studie der Washington Post vom November 2013 sind rund zwei Drittel der Amerikaner zwar tief besorgt über die staatliche Ausspähung (Washington Post 2013), aber eine große Zahl von diesen findet es zugleich richtig und wichtig, zum Beispiel den Aufenthaltsort der Kinder oder des Partners per Handy-Ortung jederzeit bestimmen zu können. Es dürfte – nebenbei

gesagt – für den Smartphone-Fan Barak Obama eine nicht gelinde Überraschung zum Amtsantritt gewesen sein, das man ihm aus Sicherheitsgründen (so wie zwei identische schwarze Limousinen und ebenso zwei identische Hubschrauber) sogar mehr als zwei (Insider sprechen von über 20) täglich jeweils zu wechselnde Smartphones verordnete. Denn aus Sicherheitsgründen darf die bestbewachte Person der Welt nicht einmal mit einem verschlüsselt sendenden Mobilgerät ihre Lokation für Dritte länger als erforderlich preisgeben.

Bei der als Schnittmenge über (oder neben) diesen beiden Gruppen stehende Netzavantgarde mag es andere Gründe geben. „Keine Empörung, zudem eine überschaubare Teilnehmerzahl" (Kurz 2013) gab es selbst bei der Initial-Demonstration des Netzsicherheit-Meinungsführers CCC in Berlin. Das seit NSA 2013 auch „real" existierende globale Spähnetz hat vielleicht deswegen die antagonistischen Nerd-Sparten neutralisiert, weil es niemanden und nichts verschont, keinen PC und keinen Apple, kein Handy und kein Smartphone, keine proprietäre und keine offene Software, kein gemeinnütziges Spendenmedium und kein verordnetes Zwangszahlermedium. Auch die mächtigste Waffe des gemeinen Netznutzers, der „fristlose Providerwechsel möglichst mit sofortiger Flatrate-Preisreduktion, aber ungedrosselt", bleibt wirkungslos im @groll Blog-Abschussbunker. Aber selbst der Netzavantgarde ist zusammen mit den beiden genannten Nutzergruppen nicht bewusst, dass ihre nachhaltigste Waffe der Mechanismus der Marktnachfrage wäre und nicht etwa ein Regulierungsmechanismus. Nur: Wenn alles am Internet nicht akzeptabel ist, dann könnte nur ein totaler Nachfrageverzicht eingesetzt werden. Nicht einmal der in seinem Internet-Glauben abgrundtief enttäuschte „Internet-Erklärer" Sascha Lobo („Das Internet ist kaputt.", Lobo 2014) erwägt eine solch radikale Empfehlung.

Auf der entgegengesetzten Seite stehen die Verfechter des „Nothing to hide", die bei der Erfassung aller Kommunikationsdaten keinerlei

Problem sehen, denn sie haben ja nichts zu verbergen. Die seit einigen Jahren in den USA laufende Diskussion über die gegenläufige Abhängigkeit von Privatheitsschutz und Sicherheit (vgl. Solove 2011) hat im Lauf der NSA-Affäre auch in Deutschland Zulauf von selbsterklärten braven Bürgern bekommen. Im Einzelgespräch mit solchen – eine repräsentative Untersuchung wäre methodisch und praktisch nicht möglich – stellte es sich in den vergangenen Monaten oft heraus, dass sich diese vor allem auf den Geheimdienst NSA bezogen. Auch ein deutscher Geheimdienst könne doch getrost alles speichern und auswerten, weil man ja diesem gegenüber erst recht nichts zu verbergen habe. Auch die nationalen Polizeien dürften doch gerne alles speichern und untersuchen, eventuell mit Ausnahme der Verkehrspolizei mit Bezug auf netztechnisch überwachte mögliche Geschwindigkeitsübertretungen. Sehr viel zurückhaltender wird die Reaktion – und dies nicht nur von Geschäftsleuten – im Zusammenhang mit den Daten der Finanzverwaltung, gekoppelt mit dem elektronischen Geldverkehr, dies würde doch wohl „allzu viel Missverständnisse gegenüber uns braven Steuerzahlern" erzeugen, wenngleich dies andererseits einen Schutz gegen Cyber-Kriminelle darstelle. Auch gezielte Werbung aufgrund eines Datenprofils sei doch überhaupt kein Problem, man müsse als mündiger Konsument das Beworbene ja nicht kaufen.

Die Zustimmung zu „behördlichen" Kontrollmöglichkeiten bricht aber abrupt in sich völlig zusammen, wenn man die Nothing-to-hide-Gruppe fragt, ob dieselben Daten auch gegenüber den Nachbarn, den Partnern, den Freunden (gar den ehemaligen Bezugspersonen) und dem Konkurrenten transparent sein dürften. Dass zum Beispiel die Lokationsdaten von SIM-Karten und IMEI-Gerätenummern durch private Dritte in anonymer Form mithilfe von Tracking-Diensten abgerufen werden können, dass der e-Call der EU Daten durchaus nicht nur für den Notfall liefert, sondern auch für Zwecke der Verkehrsüberwachung dienen kann und dass in den USA bereits permanent Car-to-X-Daten über das Fahrerverhalten die Höhe des

Fahrzeugversicherungstarifs entscheiden, lässt die Gesprächsteilnehmer verstummen. Diese unterschiedliche räumliche und zeitliche Granularität einer „Betroffenheit" kommt soziologisch nicht überraschend. Schon bei der Volkszählung vor drei Jahrzehnten gab es solche Indizien. Und wer es wissen will, kann auch (wenngleich nicht per Suchanfrage „Boykott-Initiativen" im hochgelobten Wissensnetz, vgl. Schreier 2011, 19) herausfinden, dass wahrscheinlich die meisten Volkszählungs-Boykotteure schon von 1983 die stillen Eigennutzer von (nur bei Vermietung steuerbegünstigten) Einliegerwohnungen waren, nicht die sichtbar engagierten Datenschützer. Nicht nur die schwäbischen Häuslesbesitzer klebten damals vorsorglich ein Phantasie-Namensschild (statistisch: Neubürger) an die betreffende Einliegerwohnung, sie verweigerten ihre Teilnahme aus „privaten Gründen" und spürten nichts von Fremdbestimmung.

Auch diese Nothing-to-hide-Gruppe wird absehbar nicht in ihrer radikalen Zustimmung verharren können, sondern im Laufe der weiteren Sachaufklärung Stimmen beipflichten, die nicht nur den Staat warnen: „Als Folge hat in Deutschland das Vertrauen in Staat und Wirtschaft als Garanten von Vertraulichkeit und Privatsphärenschutz im Internet deutlich abgenommen. Viele Bürger empfinden die Abhörprogramme als unverhältnismäßige Eingriffe in ihre Grundrechte und fühlen sich von ihrer Regierung allein gelassen" (Herfert/Waidner, 5). In den beiden Nutzergruppen sind zahlreich „Melioristen" (Dahrendorf) vorfindlich, die darauf vertrauen, dass die netzalltagsweltlich vorhandenen Heteronomien z. B. „durch den rasanten technischen Fortschritt" einer Besserung hin zu „datenschutz- und menschengerechten bis hin zu sozialverträglichen Produkten und Systemen" unterzogen werden. Bei gegebener instantaner Akzeptanz ist es aber auch für den vielzitierten „kreativen und innovativen Schumpeter'schen Erfinder und Unternehmer" recht schwer, das dafür heutzutage erforderliche „Business-Modell" zu finden: Wo – zurückhaltend formuliert – keinerlei Nachfrage nach höheren Produkt- und Nutzungskosten besteht, können

Verbesserungen selbst von denkbar nachdenklichen Anbietern nur kostenneutral gesucht werden. Entgegen weit verbreiteter Auffassung ist aber auch selbst die kleinste Verbesserung von Software nicht zum Nulltarif zu haben. Weltweite Verbesserungen – etwa von infrastrukturellen Standards und Verfahren – in einer Wettbewerbswirtschaft kosten sogar so viel Geld und Zeit, dass bei aller Einigkeit über die Verbesserung kein wirtschaftlicher Akteur beginnen will. Die FCC hat dies seit einigen Jahren beim immer wiederkehrenden „runden Tisch" stets aufs Neue erfahren müssen.

Das Dilemma des Handlungsbedarfs im Einerseits-Andererseits

Nach den abgeklärten Einerseits-Anderseits-Mustern in den Sichtweisen von Rechtswissenschaft, Psychologie, Soziologie, Systemtheorie und Informatik bis hin zur Ökonomie und Politik steht für das Grundrecht auf informationelle Selbstbestimmung immerhin noch die ideengeschichtliche Kontinuität der Politische Theorien als handlungsinduzierende Kraft zur Verfügung. Der Freiheitsbegriff des Liberalismus, das Fürsorgeprinzip des Konservatismus, das Solidaritätsprinzip des Sozialismus und auch das Nachhaltigkeitsprinzip des Ökologismus erbringen je für sich und erst recht zusammen solche Impulse, wobei alle nach Durchlauf innerwissenschaftlicher und innerparteilicher Diskussionen in gesellschaftlichen Selbstbindungen – sprich: kollektiver Bezahlungsnotwendigkeit – enden, für die es allerdings keinen Haushaltstitel gibt, nirgendwo in Deutschland zumindest. Und selbst ein populistischer (und damit im föderalen Durchgangsland Deutschland durchaus vorstellbarer) Vorschlag für eine Datenmautgebühr zur Ausbesserung nur der schlimmsten Daten-Schlaglöcher und Software-Korrosion brächte jeden Vorschlagenden in den sofortigen Spießruten-Boulevard mit virtuell-flexiblen Meinungsumfrage-Ergebnissen.

Technische, technologische oder innovatorische Verbesserung zielt heute überall und ausschließlich auf kostenmäßige Verbesserung, so wie sich (nur) in Deutschland der einstige Hoffnungsbegriff „Reform" innerhalb eines Jahrzehnts *konnotativ* zur Drohbedeutung „Reduktion" gewandelt hat. Die dabei unversehens in semiotische Nöte geratene römische Ziffer IV, die ironischerweise lange Zeit ein neutrales Lateinbuchstabenkürzel für „Informations-Verarbeitung" war, wird deswegen bei der nächsten Generation „Industrie 4.0" nicht mehr verwendet. Es ist für die Wirtschaftsakteure schon schwierig genug, vor der – ausschließlich von Zuwachs oder wenigstens Sicherung von Arbeitsplätzen – abhängigen Wahlpolitik die absehbaren Konsequenzen für den globalen Arbeitsmarkt möglichst opak zu halten; auch für die befasste, von Politik und Wirtschaft am Leben gehaltene Wissenschaft wäre die prognostische (mehr als lineare) Fortschreibung der Probleme mit Privatheit, Datenschutz und informationeller Selbstbestimmung ein letales Darstellungsproblem. Es dominiert in allen Subsystemen die Selbstreferentialität: „Die Organisation der nächsten Gesellschaft ist kenogrammatisch. Sie definiert Leerstellen, die jederzeit anders besetzt werden können" (Baecker 2011, 10). Die Frage, ob Begriffe wie „Digitale (smarte, intelligente, offene, transparente) Demokratie" eine sich festigende Basis angesichts klar absehbarer globaler Krisenaufwüchse darstellen können, wird zunächst aufgeschoben. Die Stoppuhr läuft allerdings unerbittlich: „Bei sich verändernder Umwelt wird ein rigides System (soziales Sinnsystem) nicht dauerhaft überleben können, da der Außendruck an der Grenze zwischen System und Umwelt nicht durch Veränderung ausgeglichen wird" (Wenzel 2012).

Und nicht überraschend rufen jetzt verantwortliche Akteure in Staat und Wirtschaft in durchaus allgemeiner Form (also ohne konkreten Projektauftrag) die Wissenschaft auf, Lösungsvorschläge zu machen. Auch wenn in der befassten Wissenschaft die Einsicht noch nicht Platz gegriffen hat, dass sich hinter dem hochinteressanten Forschungsgebiet „Big Data" ein recht abschüssiger Weg zu einem

„All Data" befindet, darf dies angesichts der eingetretenen Paralysierung von Staaten und Wettbewerbswirtschaften nicht verwundern. Verbale Bekundungen stimmen seit langem darin überein, dass es sich um ein großes und komplexes Problem handelt: „Vertraulichkeit und Privatsphärenschutz im Internet können nicht alleine auf der Ebene der Informationstechnologie adressiert werden; es sind auch Ethik, Psychologie, Soziologie, Recht und Ökonomie gefragt. Alle diese Disziplinen müssen zusammenarbeiten, um Anforderungen zu präzisieren und Lösungen zu entwickeln" (Herfert/ Waidner, 6). Hinter der Forderung nach ganzheitlichen Lösungen steht konsequent auch die Haltung „Wir müssen das Netz neu erfinden", wie sie Tim Pritlove zu Beginn des Chaos Computer Kongresses (30C3) in Hamburg am 27. Dezember 2013 formulierte.

Wilhelm Steinmüller hatte dabei schon auf ein Grundproblem hingewiesen: „Namentlich in der WI herrschen zum Verhältnis von Datenschutz, Datensicherung und Datenschutzrecht auch bei renommierten Autoren unklare und z. T. abenteuerliche Vorstellungen, wie ein Überblick über die Lehrbücher zeigt" (Steinmüller 1993, 703). Ebenso klar waren seine Zweifel „Erst recht sind die Möglichkeiten einer vertieften Humanisierung der Telematik durch datenschutzkonforme Technikgestaltung nicht ins allgemeine Bewußtsein oder auch nur in die Kompetenz der Experten gelangt" (ebda, 700). Eine Voraussetzung für interdisziplinäre Ansätze ist das fachbereichsübergreifende Verstehen, das beim Blick zurück nicht gegeben war: „Bei der ISDN-Normung war weder in der Wissenschaft, noch bei Herstellern und Betreibern auch nur hinreichendes Wissen um Kommunikationssoziologie und -psychologie vorhanden" (Klumpp 1990, 58).

Mit der „Legendenbildung um ISDN als Prozess wechselseitiger Missverständnisse" (Klumpp 1991, 176) befasste sich einer der wenigen Diskurse zwischen kritischer Wissenschaft und der Telekommunikationsbranche. Das Hauptaugenmerk galt dabei der mit der

digitalen Vermittlungstechnik seit 1982 möglichen Anzeige der Rufnummer des A-Teilnehmers beim B-Teilnehmer. Die dafür technisch zugrunde liegende Kommunikationsdatenerfassung (KDE) für den Gebührennachweis des Betreibers war schon seit Herbst 1977 nach Abstimmung auch mit dem Bundeskriminalamt im Zuge des G10-Regelwerks durch die Vorschrift richterlicher Kontrolle gleichsam rechtskonform. Der entscheidende Unterschied der digitalen KDE gegenüber der vorherigen analogen Vermittlungstechnik lag darin, dass im Kontrollfall bei einem Anfangsverdacht der Ermittler nur die Telefonnummer des Verdächtigten und deren Verbindungen erfasst wurde, in der digitalen Vermittlung hingegen sämtliche Telefonverbindungen in einer Vermittlungsstelle sozusagen auf Vorrat gespeichert werden konnten und wurden. Die beiden deutschen Digitalsysteme folgten hier dem Muster der schon zehn Jahre vorher entwickelten Digitalsysteme der USA und Frankreichs. Schon 1983 gab es Hinweise, dass der gesamte Überseetelefonverkehr Englands auf Reizworte hin untersucht werde, was damals jedoch wohl die Kapazität aller in England existierenden Computer um ein Mehrfaches überstiegen hätte. Doch dreißig Jahre später steht diese erforderliche Computerkapazität sogar im Übermaß zur Verfügung, so dass es nicht nur möglich wurde, eine Kontrolle der gesamten Telekommunikation auf Schlüsselworte hin zu untersuchen, sondern sogar mithilfe von Algorithmen per Data Mining auf alle nur erdenklichen Auffälligkeiten zu stoßen. So betrachtet, wurde aus dem (richterlich kontrollierten) Anfangsverdacht von computerunterstützten Ermittlern gegenüber *einzelnen* Teilnehmern gleichsam ein durch Software-Algorithmen herausgefilterter Anfangsverdacht gegenüber *vielen und sogar allen* Teilnehmern, mit dessen Bewertung sich dann erst die Ermittler zu befassen hatten, bevor eine richterliche Instanz ins Spiel kommen konnte.

Wenig beachtet wird bis heute die damalige Entscheidung der USA, dass eine europäische Systemdefinitionshoheit wie bei ISDN für eine Supermacht keinesfalls akzeptabel sein könne. Dies hatte

klare Folgen für die entstehende globale Netz-Architektur: „So ist eines der Grundprinzipien des paketvermittelnden Internets die Zustellung von Datenpaketen, ohne dass der Empfänger sein Einverständnis gegeben haben muss (anders als bei leitungsvermittelnden Diensten, bei denen ein Verbindungsaufbauwunsch abgelehnt werden kann). (…) Ein wirkungsvoller Schutz gegen bandbreitenerschöpfende DoS-Angriffe ist nur beschränkt möglich“ (Schäfer/Rossberg 2014, 13). Es ist nicht verwunderlich, dass mit dem Mobilfunksystem GSM, das im Rahmen von EUREKA 1984 von Deutschland und Frankreich vorangetrieben wurde, bislang letztmalig eine nicht-amerikanische Systementwicklung zum Zuge kam. Wie sich die Supermacht USA nach dem Verschwinden europäischer Systementwicklung mit japanischen, koreanischen oder chinesischen Systementwürfen verhalten werden, sei dahingestellt.

Die Wissenschaft in Deutschland legt in der Tat bereits interdisziplinäre Ansätze für sozial- und rechtsgemäße Gestaltung vor: „Informationelle Selbstbestimmung und Telekommunikationsgeheimnis müssen durch Infrastrukturen unterstützt werden, die ermöglichen, auf Gefährdungen automatisch zu reagieren, ohne dass dies aufdringlich oder belästigend wirkt. Die Erfüllung rechtlicher Vorgaben muss in die Techniksysteme integriert sein (Privacy by Design).“ (Roßnagel 2014, 23). Richtig erkannt ist: „Rechtlicher Schutz endet an den Grenzen Deutschlands oder Europa, Grundschutzrecht durch Technik wirkt dagegen global.“ (ebd., 23) und „Schließlich hat technischer Nutzerschutz gegenüber rechtlichem Nutzerschutz gewisse Effektivitätsvorteile: Was technisch verhindert wird, muss nicht mehr verboten werden“ (ebd., 18). Diese einfachen Leitbilder können jedoch nicht mehr für das gesamte Internet mit seiner gewachsenen (nicht durchweg gestalteten) Infrastruktur und Netzarchitektur gelten, sondern nur für künftige Entwicklungen der Netz- und Gerätetechnik samt der Kommunikationsdienste.

Rahmenbedingungen für (oder gar Einflussnahme auf) technologische Entwicklungen oder ganze Netzarchitekturen sind also nach aller Erfahrung nur in ihrer Anfangsphase möglich. Software-Ingenieure und Technikwissenschaftler sind in diese Phase mit der „technologischen" (gemeint ist meist „technischer") Entwicklung als solcher beschäftigt. Für die Ökonomen zeigt sich in dieser Phase noch wenig statistisch Erfassbares im empirisch messbaren Marktmechanismus von Angebot und/oder Nachfrage. Auch die Juristen (mit graduellen Unterschieden im angloamerikanischen und kontinentalen Recht infolge der „Präzedenz") sehen Handlungsbedarf erst bei Vorliegen eines Sachverhalts. Politiker aller Parteien sehen Handlungsbedarf sogar erst beim breiten Bekanntwerden eines problematisch erscheinenden Sachverhalts in der Wahlbevölkerung.

Ob es in Deutschland bzw. aus Deutschland angesichts der beschriebenen Akzeptanzmuster zu einer solchen diskursiven Gestaltungsanforderung kommt, steht dahin. Denn es darf nicht weiterhin übersehen werden, dass selbst nach einer „politischen" Entscheidung Deutschland (wie auch Europa insgesamt) für nahezu jedwede Hard- und Software ein Nettoimporteur ist und absehbar bleiben wird. Bei gegebener Akzeptanz, der „Abstimmung der Käufer an der Wahlurne des Marktes" (in den Worten eines F.A. von Hayek) wird plausiblerweise nichts anderes geliefert. Dies gilt nicht nur für Konsumprodukte, sondern auch und gerade für Infrastrukturen, deren Technik, deren Organisation und deren Enkulturation. Das einzig denkbare Gestaltungsargument wäre das absolute Volumen des deutschen Marktes, wenn es denn gelänge, diese Nachfragemacht zu bündeln und einen klaren „Innovationsrahmen" (vgl. im Web: innovationsrahmen.de) für alle globalen Anbieter zu ziehen.

Die mit der „Informatisierung" in vier Jahrzehnten entstandene Softwarewelt weist tatsächlich Charakteristika auf, deren Risiken (im Neusprech: Herausforderungen) für die Entwicklung von Gesellschaften vor allem wegen ihrer Undurchschaubarkeit und ihrer

permanenten Replikationsmöglichkeit als kategorial *neuartig* bezeichnet werden können. Es hat in der Menschheitsgeschichte keine Zeit gegeben, in der die Chance der Bewahrung wie die Chance des Vergessens von Daten, Information und Wissen gleichermaßen unmöglich war. Die informationelle Selbstbestimmung des Menschen hat mit der laufenden Entwicklung auf dem Weg hin zu einem Zustand „All Data" einen neuen fremdbestimmten Widerpart erhalten.

Literatur

Baecker, Dirk, Zukunftsfähigkeit: 16 Thesen zur nächsten Gesellschaft, in: Revue für postheroisches Management, Heft 9 (2011), S. 9–11.

Baum, Gerhart, Rettet die Grundrechte! – Bürgerfreiheit contra Sicherheitswahn, Köln 2009.

Baum, Gerhart, Ich will, dass wir beißen können, in: Frankfurter Allgemeine Feuilleton vom 24.9.2013.

Borchers, Detlev, Vor 30 Jahren: Das Volkszählungsurteil macht Geschichte, in: heise online news, 15.12.2013.

Elster, Jon, Die Subversion der Rationalität, New York 1987.

Capurro, Rafael (2014), vgl. mit zahlreichen Verweisen: http://www.capurro.de/infoethik_standort.htm.

Gauck, Joachim, „Die Freiheit in der Freiheit gestalten", in: http://www.bundespraesident.de/SharedDocs/Reden/DE/Joachim-Gauck/Reden/2013/10/131003-Tag-deutsche-Einheit.html.

Herfert, Michael; Waidner, Michael, Privatsphärenschutz und Vertraulichkeit im Internet. Trend- und Strategiebericht, Darmstadt, 16.9.2013.

Horchert, Judith, Zur Freiheit gehört die Chance des Vergessens, Interview mit Johannes Mading, in: Spiegel Online v. 31.1.2014.

Hoffmann-Riem, Wolfgang, „Der Staat muss Risiken eines Missbrauchs durch Infiltrierung vorbeugen", in: FAZ v. 9.10.2011.

Kammer, Matthias, Hier wartet unerledigte Arbeit. Wir haben ein Recht auf Klarheit in der Schnüffel-Affäre, in: DIVSI magazin, Dez. 2013, S. 24 ff.

Klumpp, Dieter, Technikfolgenabschätzung: Bedingungen und Perspektiven in der kommunikationstechnischen Industrie, Stuttgart 1989, in: Mai, Manfred (Hrsg.), Sozialwissenschaften und Technik – Beispiele aus der Praxis, Bern, Frankfurt, New York, 1990 S. 45–83.

Klumpp, Dieter, Die Legendenbildung um ISDN als Prozeß wechselseitiger Mißverständnisse, in: Kubicek; Noam; Roßnagel; Schnöring; Welsch et al. (Hrsg.), Telekommunikation und Gesellschaft, Kritisches Jahrbuch der Telekommunikation, Karlsruhe 1991.

Kurz, Constanze, Aus dem Maschinenraum, Die neue Dimension des Duckmäusertums, in: http://www.faz.net/aktuell/aus-dem-maschinenraum-die-neue-dimension-des-duckmaeusertums-12708250.html vom 12.12.2013.

Lobo, Sascha, Das Internet ist nicht das, wofür ich es gehalten habe, in: Frankfurter Allgemeine Sonntagszeitung vom 12.1.2014.

Müller, Günter; Pfitzmann, Andreas (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, Verfahren, Komponenten, Integration, Bonn/ Reading u. a. 1997.

Roßnagel, Alexander (Hrsg.), Nutzerschutz, Rechtsrahmen, Technikpotentiale, Wirtschaftskonzepte, Baden-Baden 2012.

Roßnagel, Alexander, Persönlichkeitsschutz in einer vernetzten Welt. Grundrechte und Datenschutz, in: VDE-Dialog, Frankfurt am Main 2014, S. 20–23.

Schäfer, G.; Rossberg, M., Netzwerke schützen – aber wie?, in: VDE-Dialog, Frankfurt am Main, 2014. S. 12–15.

Schulz, Sönke, Ist das Grundgesetz tauglich für die digitale Zeit? In: DIVSI magazin, Dez. 2013, S. 24 ff.

Schwartz, Paul M., EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation, in: Privacy & Security Law Report, 12 PVLR 718, 04/29/2013.

Schreier, Christian, Die Massenverfassungsbeschwerde beim Bundesverfassungsgericht. Versuche der Revision von Rechtsnormen durch Bürgerinitiativen, Opusculum Nr. 51, November 2011.

Solove, Daniel J., Nothing to Hide: The False Trade-off between Privacy and Security, New Haven 2011.

Steinmüller, Wilhelm (Hrsg.), Verdatet und vernetzt, Sozialökologische Handlungsspielräume in der Informationsgesellschaft, Frankfurt 1988.

Steinmüller, Wilhelm, Informationstechnologie und Gesellschaft: Einführung in die Angewandte Informatik, Darmstadt 1993.

Washington Post, Surveillance in America – Washington Post Poll November 2013 Government and corporate surveillance draw wide concern, Published: December 22, 2013.

Wenzel, Joachim, Eine Einführung in die Systemtheorie selbstreferentieller Systeme nach Niklas Luhmann, Mainz 2012.