Thilo Weichert

Netzwerk Datenschutzexpertise

Security Forum – 19. Januar 2017

Technische Hochschule Brandenburg

Keynote **Demokratie 4.0**

Als mich vor Weihnachten für die Veranstalter des Security Forums Prof. Holl kontaktierte und mir mitteilte, dass als Keynote-Speaker Justizminister Heiko Maas für das Thema „Demokratie 4.0“ ausfällt und ob ich diesen Part übernehmen könne, habe ich spontan zugesagt. Zwar meine ich nicht, Heiko Maas vertreten zu können. Doch zum Thema gibt es vieles zu sagen. Ich teile dabei wohl nicht in jeder Hinsicht die Meinung des Justizministers.

Demokratie 4.0 übersetze ich mit Demokratie in einer und in unserer modernen, globalisierten hochtechnisierten Informationsgesellschaft. Zur Demokratie gehören für mich dabei nicht nur Mehrheitsentscheidungen in Volksabstimmungen oder Wahlen. Mit Mehrheiten können auch Autokraten, die Todesstrafe oder eine Parlamentsentmachtung bestätigt werden. Zu Demokratie gehören für mich auch die Gewährleistung von Freiheits- und Minderheitenrechten, die Gewaltenteilung und eine rechtsstaatliche Kontrolle durch unabhängige Gerichte.

Mit einem solchen Demokratieverständnis sind wir als Europäer in der Welt ziemlich einsam. Nicht nur China, Saudi-Arabien, der Iran oder Russland sind davon weit entfernt, sondern auch sog. befreundete Staaten wie z. B. die USA. Mit einem solchen Verständnis sind wir aber auch innerhalb Europas nicht einer Meinung. Was Demokratie in unseren Informationsgesellschaften in der Mitte Europas bedeutet, ist alles andere als Konsens, ist hochumstritten. Über Demokratie 4.0 haben viele unserer Regierenden, unserer Parlamentarier und unserer Richter noch nicht richtig nachgedacht.

Erfahrungen aus der Geschichte

Im 15. Jahrhundert schuf Johannes Gutenberg mit der Verbreitung des Drucker-Mediums eine zentrale Voraussetzung für die Aufklärung und für die demokratische Verfasstheit unserer Gesellschaften in Europa. Mit den Informations- und Kommunikationsmedien und insbesondere über das Internet hofften dann viele von uns noch vor knapp 10 Jahren, könnte eine weitere Stufe der Demokratisierung erklommen werden. Der freie Meinungsaustausch und freie Informationen im Netz würden es schon richten. Während

des sog- arabischen Frühlings vor 6 Jahren meinten dann gar einige, dass die modernen Kommunikationsmedien die feudalen Gesellschaften nachhaltig und nicht mehr rückholbar in ein demokratisches Zeitalter befördern würden. Verblüfft mussten wir dann feststellen, dass das Gegenteil der Fall war, dass mit Hilfe der technisch plötzlich machbaren Überwachungs- und Manipulationsinstrumente die sprießenden liberalen Pflänzchen zertreten wurden. Wir mussten und müssen – am offenbarsten bei Beispielen wie China, Russland, Iran, aber auch Syrien – zur Kenntnis nehmen, dass Diktaturen oder totalitäre Staaten hervorragend mit modernen Informationstechniken zurechtkommen und dass diese sehr gut zusammenpassen. Die marxistische wie die neoliberale Hoffnung, dass der technische Fortschritt letztlich – quasi automatisch – zum Wohl und Nutzen aller führt, erweist sich als eine naive Illusion.

Es hat sich also nichts daran geändert, dass die digitale wie jede Demokratie von Menschen erkämpft werden muss und dass dieser Kampf oft blutig, in jedem Fall aber oft frustrierend und nie endgültig endschieden ist.

Für mich trug Evgeny Morozov mit seinem 2011 erschienen Buch „The Net Delusion“ stark dazu bei, dass ich mir keine Illusionen mehr über digitale Heilsbotschaften mache. 2016 konnten wir nun aus der Nähe und in der Ferne in modernen westlichen Gesellschaften miterleben, wie Demokratie mit digitalen Werkzeugen beschädigt werden kann: Sowohl die Brexit- wie auch die US-Präsidentschaftskampagne waren anschauliche Lehrbeispiele, wie mit Desinformationen und Hasspostings in sozialen Netzwerken sich radikale Stimmungen hochschaukelten, und wie eine kritische Berichterstattung als Lügenpresse diffamiert wurde. In hermetisch wirkenden Filterblasen, in denen demokratischer Diskurs oft unmöglich ist, wurde und wird die Spaltung der Gesellschaft betrieben. Über Social Bots, die z. B. im US-Wahlkampf aus einem Dorf in Mazedonien befeuert wurden, wurde die Stimmung weiter angeheizt. Diese Phänomene beschränken sich nicht auf die USA und Großbritannien. Sie sind in Europa allgegenwärtig und prägten den österreichischen Präsidentschaftswahlkampf ebenso wie die Flüchtlingsdebatte und die Landtagswahlen 2016 in Deutschland.

Ein weiteres aufschlussreiches Phänomen war im US-Wahlkampf gut erkennbar: Mit Hilfe von sog. Psychometrik oder Psychografie wurden die Menschen in sozialen Medien nach fünf Persönlichkeitsdimensionen – Offenheit, Gewissenhaftigkeit, Extraversion, Verträglichkeit und Neurotizismus – digital vermessen und dann informationell mit passgerecht gemachten Meinungen bearbeitet, bei denen es auch nicht auf faktische Richtigkeit und schon gar nicht auf Verträglichkeit mit humanitären Prinzipien ankam. Das grundsätzliche Vorgehen ist altbekannt. Vance Packard beschrieb 1957 es in seinem Buch „Die heimlichen Verführer“ – ein Buch, das ich als Jugendlicher gierig verschlungen habe. In zweierlei Hinsicht haben wir aber seit den 50er Jahren heute Weiterentwicklungen: 1. Die Verführungen sind diesmal politisch und nicht mehr nur kommerziell. 2. Diese werden nicht mehr unter den Augen der Öffentlichkeit an einen Massenmarkt adressiert, sondern auf der Grundlage geheimer Algorithmen und an der Öffentlichkeit vorbei in Form personalisierter Ansprache.

Wir haben in Deutschland unsere eigenen Erfahrungen mit modernen Informations- und Kommunikationsmedien und deren Einsatz gegen die Demokratie gemacht: Die

Nationalsozialisten bedienten sich in den 30er und 40er Jahren der damals neuen Rundfunktechnik für Ihre Propaganda, um eine Gesellschaft autoritär zu programmieren und gleichzuschalten und um Minderheiten und Freiheitsrechte auszuschalten. Mich verblüfft, wie wenig diese Erfahrungen bei der Bewältigung der heutigen medialen Probleme herangezogen werden, könnten wir doch von damals einiges lernen. Der Nationalsozialismus benutzte nicht nur den Rundfunk, sondern auch andere damals moderne informationelle Herrschaftsmedien zur Zerstörung der Weimarer Demokratie. Ein Instrument waren die Geheimdienste, insbesondere die mit der Polizei verschmolzene GeStaPo. Ein weiteres Instrument war die lückenlose Bevölkerungserfassung, insbesondere auch der sog. fremdvölkischen Menschen, der Juden, der Sinti/Roma und der Osteuropäer. Dieses Erfassungsinstrument wurde mit bürokratischer Akribie für die Organisation von Zwangsarbeit bis hin zur Menschenvernichtung und zum Völkermord in den Konzentrationslagern genutzt.

Eine historische Antwort auf die Gräuel des Nationalsozialismus war unser Grundgesetz mit seinen Freiheits- und Grundrechten. Die darin gezogenen Lehren waren zunächst vor allem organisatorisch, rechtlich und materiell. Die Aufarbeitung und Analyse der informationellen Herrschaft der Nazis erfolgte erst erheblich später in den 70er und 80er Jahren und fiel in die Zeit der Planung einer bundesweiten Volkszählung. Unsere modernen informationellen Grundrechte verdanken wir dieser Aufarbeitung, die zum Volkszählungsurteil des Bundesverfassungsgericht im Jahr 1983 führte, mit dem ein Grundrecht auf informationelle Selbstbestimmung abgeleitet, besser gesagt „erfunden“ wurde.

Informationelle Grundrechte

In dieses Urteil schrieben die Verfassungsrichter eine vielzitierte Passage hinein, die weiterhin und wohl noch in tausend Jahren Gültigkeit hat:

„Individuelle Selbstbestimmung setzt (…) – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des

Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.

Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus."

Diese Ausführungen des BVerfG haben schon der damaligen Bundesregierung nicht gefallen. Inzwischen hat das BVerfG in vielen Entscheidungen die zitierten Ausführungen präzisiert und auf spezifische Normen und Situationen angewendet. Immer wieder ist es dabei zu dem Schluss gekommen, dass politische Entscheidungen – etwa zum Lauschangriff, zur Vorratsdatenspeicherung oder zum Bundeskriminalamtsgesetz – verfassungswidrig sind. Seit 2009 ist nun das Recht auf Datenschutz europaweit in Artikel 8 unserer Grundrechte-Charta anerkannt.

Dies hinderte und hindert weiterhin – vor allem populistische – Politiker nicht daran, weiterhin mehr undifferenzierte Überwachung und Kontrolle zu fordern. Zulässig sind aber nur normenklare verhältnismäßige Regelungen und Praktiken, die den wesentlichen Kern unserer Grundrechte wahren. Der Europäische Gerichtshof stellte in seinem Urteil vom 21.12.2016 zur Vorratsdatenspeicherung klar, dass eine allgemeine und unterschiedslose Vorratsspeicherung mit dem Argument der Kriminalitätsbekämpfung nicht gerechtfertigt werden kann, insbesondere wenn keine Differenzierungen, Einschränkungen oder Ausnahmen in Hinblick auf das verfolgte Ziel, die betroffenen Personen, die elektronischen Kommunikationsdienste, den geografischen Raum, den Zeitraum oder Berufsgeheimnisse gemacht werden. Nötig ist immer die Kontrolle, ob Datenverarbeitungen die Grenzen „des absolut Notwendigen" überschreiten und als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden können.

Die Macht der IT-Unternehmen

Während jedoch die staatlichen Gefährdungen für unsere freiheitliche Demokratie in Europa von den obersten Gerichten unter Kontrolle gehalten werden, ist dies hinsichtlich der Gefährdungen durch private Wirtschaftsunternehmen – noch – nicht der Fall. Facebook und Google beherrschen mit ca. 80% Marktanteil den globalen Online-Werbemarkt und damit die zentrale Einnahmequelle im Bereich der Informationstechnik.

Facebook hat mit ca. 1,6 Milliarden Nutzenden, das sind etwa ein Siebtel der Weltbevölkerung, mehr Mitglieder als der weltweit größte Staat – China – Einwohner. Über 27 Mio. aktive Nutzende, ca. 1/3 der deutschen Bevölkerung, wovon sich 78% täglich einloggen sollen, hat Facebook detaillierte Kenntnisse zu Kommunikation und Lebensgewohnheiten. Hinzu kommt das Wissen über die Nichtmitglieder, die von Facebook mit Hilfe von Cookies auf anderen Webseiten über sog. Like-it-Buttons erfasst werden. Facebook hat im Jahr 2015 seinen Gewinn auf 1,5 Mrd. Dollar gegenüber dem Vorjahr verdreifacht und den Umsatz auf 53,8 Mrd. Dollar gesteigert. Bisher waren keine kritische Öffentlichkeit, keine demokratische Instanz, kein Gericht und keine Behörde in

der Lage, Licht in die Aktivitäten der Datenerfassung und Auswertung zu bringen, geschweige denn diese zu kontrollieren oder zu lenken. Es ist für einen Rechtsstaat und eine Demokratie absurd, dass solche einflussreichen Unternehmen es bis heute schaffen, ihre Profite ohne wesentliche Steuerabführungen zu machen, dass deren Monopolisierungsbestrebungen kaum auf behördlichen kartellrechtlichen Widerstand stoßen und dass deren Geschäftsmodell seit Jahren auf informationeller Fremdbestimmung der Internetuser unter Verletzung grundlegender Datenschutzregeln erfolgreich praktiziert wird.

Demokratie bedeutet, dass, so Artikel 20 unseres Grundgesetzes, dass alle Staatsgewalt grundsätzlich vom Volke ausgehen muss. Unser Gesellschaftsvertrag basiert darauf, dass dem Staat das Gewaltmonopol zukommt und dass es Privatunternehmen nicht zusteht, Teile dieser Funktion zu übernehmen.

Es ist jetzt nicht so, dass das Silicon Valley gezielt dazu beitrug, dass Trump zum US-Präsident gewählt wurde. Dieses Ergebnis dürfte auch dort den meisten – mit relevanten Ausnahmen wie dem Investor Peter Thiel – eher unheimlich sein. Dennoch: Die von den IT-Unternehmen etablierte, unkontrollierte informationstechnische Infrastruktur war eine zentrale Voraussetzung für Trumps Wahlerfolg und für viele weiteren Gefährdungen für unsere Demokratie.

Übrigens: Es ist ausgemachter Unsinn, die Trump-Wahl der russischen Regierung anzulasten. Es mag sein, dass von der russischen Regierung initiiert oder geduldet, Hacker die Partei der „Demokraten“ ausspioniert haben und deren Kommunikation u. a. über Wikileaks veröffentlichen ließen. Relevant, geschweige denn entscheidend war dies nicht. Die aktuelle Kampagne der morgen sich verabschiedenden Obama-Administration diente – voraussichtlich erfolglos – ausschließlich dem politischen Zweck, Trumps Annäherung an Russland zu behindern.

Fakt bleibt aber, dass IT-Unternehmen der eigene kurz- und mittelfristige Profit näher liegt als die Bewahrung unserer Demokratie, unserer Meinungsfreiheit und des offenen Diskurses, als die Verteidigung der Persönlichkeitsrechte und der digitalen Souveränität von Staat und Bürgern.

Genau aus diesem Grund verweigern diese Unternehmen – die angeblich angetreten sind, die Welt transparenter zu machen – jeglichen Einblick in ihr Handeln. Deshalb schöpfen sie alle juristischen Möglichkeiten aus, um nicht wegen ihrer Datenschutzverstöße zur Verantwortung gezogen, an ihren Konzentrationsbestrebungen gehindert oder bei ihren Steuervermeidungsstrategien gestoppt zu werden.

Unsere Politik

Tatsächlich gibt es wenige Politiker, die diese unternehmerische Anarchie unter Kontrolle bekommen wollen. Zu diesen gehört auf europäischer Ebene die frühere Kommissarin Vivian Reding, die eine europäische Datenschutzgrundverordnung auf den Weg brachte; zu ihnen gehört auch Margrethe Vestager, die gegen die Steuervermeidungs- und

Kartellbildungsbestrebungen kämpft.

Diesen wenigen VerteidigerInnen einer digitalen Demokratie stehen viele politische Verantwortliche gegenüber, die weiterhin ins Silicon Valley pilgern und sich als Totengräber unserer Demokratie betätigen. Zu diesen Totengräbern gehören auf europäischer Ebene verantwortliche EU-KommissarInnen sowie praktisch die gesamte Bundesregierung.

Es sind Politiker wie Günther Oettinger, Vera Jourova oder Andrus Ansip, die z. B. im Juli 2016 mit dem sog. EU-US-Privacy-Shield den US-Unternehmen – unter Missachtung der Rechtsprechung des Europäischen Gerichtshofes – einen Freibrief ausgestellt haben, ihre datenschutzwidrigen Geschäftsmodelle weiter zu betreiben. Es sind Politiker wie Angela Merkel, Siegmar Gabriel oder Alexander Dobrindt, die auf den sog. IT-Gipfeln 2015 und 2016 das hohe Lied von Big Data und den Abgesang auf den Datenschutz – etwa Zweckbindung und Datensparsamkeit – anstimmten.

Kein Schwarz-Weiß

Was ist zu tun? Zunächst ist es für BürgerrechtlerInnen zentral anzuerkennen, dass Demokratie staatliche Kontrolle bedingt. Diese banale Wahrheit hat z. B. die Piratenpartei bis heute nicht verstanden, deren wesentliche Protagonisten immer noch einer Traumwelt des kontrollfreien globalen Netzes anhängen, das frei von staatlicher Einmischung bleiben müsse. Wegen dieser Realitätsverweigerung hat diese Partei ihre historische Rolle verpasst. So wie die Grünen in den 80er Jahren als parlamentarischer Katalysator des Umweltschutzes wirkten, hätten die Piraten die digitalen Freiheitsrechte und die digitale Demokratie befördern können. Die Partei konzentrierte sich aber – was zweifellos ehrenvoll ist – auf Einzelaktionen, etwa wenn sie mit ihrer Liquid Democracy neue digitale demokratische Entscheidungsformen ausprobierten. Dass diese derzeit (noch) nicht auf große politische Systeme zu übertragen sind, hat das Bundesverfassungsgericht im Jahr 2009 mit guten Gründen dargelegt.

Staatliche Kontrolle über die digitale Infrastruktur ist dringend geboten im Hinblick auf den Schutz unserer digitalen Freiheiten. Dies setzt auch eine kurzfristige Speicherung von Telekommunikations-Verkehrsdaten voraus, wie der EuGH richtig im Oktober 2016 entschieden hat. Ohne derartige Daten lassen sich digitale Angriffe – seien diese nun gegen die Funktionsfähigkeit von IT-Diensten, gegen die Persönlichkeitsrechte der Nutzer und Betroffenen oder über Identitätsdiebstahl gegen den Inhalt von deren Geldbeutel gerichtet – nicht erkennen und abwehren. Bei der staatlichen Kontrolle des Internets müssen aber, wie das Bundesverfassungsgericht und der EuGH immer wieder darlegten, die Grundrechte auf Datenschutz und unbeobachtete Telekommunikation sowie alle weiteren Grundrechte gewahrt werden. Dies gelang nicht bei der im Herbst 2015 erneut beschlossenen TK-Vorratsdatenspeicherung. Dies gelingt auch nicht bei der derzeit geplanten Ausweitung der Videoüberwachung. Dies gelingt nicht bei den aktuellen Planungen zur Netzüberwachung durch den Bundesnachrichtendienst. Dies gelingt auch nicht durch eine Totalkontrolle aller digitalen Finanztransaktionen selbst im Bereich von Bagatellbeträgen, so wie dies derzeit die EU unter dem Vorwand der Bekämpfung von Geldwäsche und Terrorismusfinanzierung durchzusetzen versucht. Dies

gelingt erst recht nicht mit der von Innenminister de Maizière geplanten Abwehrzentrale gegen Desinformation.

Transparenz

Die zentrale demokratische Aufgabe besteht darin, die ökonomische, politische und sonstige faktische Macht der dominierenden IT-Unternehmen nicht nur zu beschränken, sondern zu brechen. Eine zentrale Bedingung hierfür ist das Einfordern umfassender Transparenz. Diese bezieht sich auf Finanztransaktionen, mit denen Steuern vermieden werden, ebenso wie auf Absprachen und Unternehmensaufkäufe, auf den Lobbyeinfluss gegenüber Politikern ebenso wie auf die Steuerung der Netzinhalte mit auf Profit programmierten Algorithmen.

Insofern haben wir hier in Deutschland ein verfassungsrechtliches Problem: Zwar hat sich in den 2000er Jahren nach langem politischen Zögern das Informationsfreiheitsrecht in der öffentlichen Verwaltung weitgehend durchgesetzt. Entsprechende Gesetze verweigern inzwischen nur noch Bayern, Hessen, Niedersachsen und Sachsen. Doch hat das BVerfG bis heute nicht anerkannt, dass in einer digitalen Informationsgesellschaft Verwaltungstransparenz eine zentrale Funktionsbedingung unserer Demokratie ist und letztlich aus den Informationsansprüchen des Artikels 5 GG, der Meinungs- und Informationsfreiheit gewährleisten soll, abgeleitet werden muss. Dass dieser Transparenzbedarf sich auch auf mächtige Wirtschaftsunternehmen bezieht, ist erst recht nicht verfassungsrechtlich akzeptiert, geschweige denn in Form von gesetzlichen Regelungen gedeckt. Vielmehr hat der Bundesgerichtshof noch jüngst das Funktionieren von Menschen existenziell tangierenden Scoring-Algorithmen zu Betriebs- und Geschäftsgeheimnissen erklärt, die nicht nur durch das Eigentumsrecht, sondern gar durch die Meinungsfreiheit von Wirtschaftsunternehmen – hier der Schufa – geschützt seien.

Das Problem fehlender Transparenz potenziert sich durch neue Formen des Big Data und der sog. künstlicher Intelligenz. Dabei handelt es sich um Computersysteme, die auf Basis von programmiert z. B. über Sensoren erfassten Erfahrungen und vielen weiteren Datenquellen eine Selbstprogrammierung vornehmen. Diese Algorithmen treffen dann Entscheidungen. Das Thema wurde in Wissenschaft und Öffentlichkeit bisher fast nur unter dem Aspekt der Haftung für Fehlentscheidungen diskutiert, etwa wenn das selbstfahrende Tesla-Auto einen tödlichen Unfall verursacht, weil es einen auf der Straße querstehenden LKW für ein Werbeplakat hielt.

Gesellschaftlich und für unsere Demokratie viel problematischer sind autonome Computersysteme, die nicht nur individuelle, sondern kollektiv relevante Entscheidungen treffen. Diese waren in unserer Demokratie bisher immer Menschen vorbehalten, die – unter Beachtung bestimmter Grundwerte und Verfahrensregeln – bei wichtigen Fragen mehrheitlich, in jedem Fall aber verantwortlich entscheiden und entscheiden müssen. Auch solche Entscheidungen werden aber heute schon und künftig zunehmend auf Computer übertragen. Begünstigt wird diese Entwicklung dadurch, dass sich hier für die IT-Industrie ein gewaltiges Geschäftsfeld auftut. Die Politik zeigt keine Neigung, regulierend tätig zu werden, zumal damit Prozesse automatisiert werden können, für die

man als Politiker keine individuelle Verantwortung übernehmen möchte. Der Versuch, das Problem allein mit sog. Computerethik in den Griff zu bekommen, muss scheitern. Hier ist nicht nur Ethik, sondern hier ist Regulierung geboten. D. h. per Gesetz müssen sozial relevante Prozesse, bei denen selbstlernende Algorithmen zum Einsatz kommen dürfen, präzise beschrieben und kontrolliert werden. Von Computer zu treffende Wertungsentscheidungen sind völlig auszuschließen.

Datenschutz und andere Rechtsgebiete

Wie vom Bundesverfassungsgericht und vom EuGH ausgeführt, ist ein funktionierender Datenschutz eine Funktionsbedingung für eine freiheitliche und demokratische Informationsgesellschaft. Lange Zeit war ein Grunde für ein weitgehendes Scheitern des Datenschutzes, dass die Politik und die Rechtsprechung sich weigerten, die Verantwortlichkeit der großen internationalen IT-Portalanbieter für Inhalts- wie auch Verkehrsdatenverarbeitung anzuerkennen. Es bedurfte des EuGH, um insofern Klarheit zu schaffen. Endgültige Klarheit, verbunden mit hinreichenden Sanktionsmöglichkeiten bringt insofern die vom europäischen Gesetzgeber beschlossene und ab 2018 direkt anwendbare Datenschutz-Grundverordnung.

Was wir aber nun derzeit auf nationaler Ebene erleben, ist eine politische Kehrtwende: Mit dem Umsetzungsgesetz zur Datenschutz-Grundverordnung versucht die Bundesregierung, die modernen innovativen Möglichkeiten eines wirksamen Datenschutzes zu sabotieren, etwa, indem die Kontrollrechte und Sanktionen eingeschränkt werden und die Betroffenenrechte beschnitten werden. Viele Bundesländer flankieren diesen Generalangriff auf den Datenschutz mit einer katastrophalen Ausstattung ihrer Aussichtsbehörden. Eine weitere von Bund und Ländern verfolgte Strategie zum Zurückdrängen des Datenschutzes besteht darin, die Leitungen der Aufsichtsbehörden mit völlig fachfremden Menschen zu besetzen.

Während im Datenschutzrecht die Weichen in Europa weitgehend richtig gestellt wurden und nun der Vollzug gefordert ist, bestehen in den Bereichen des Kartell-, generell des Wettbewerbs- und des Steuerrechts noch gewaltige rechtliche Defizite, um das globale unkontrollierte Vorgehen von IT-Konzernen unter Kontrolle und in den Griff zu bekommen. Das Problem hierbei ist, dass selbst in Europa einzelne Länder im Interesse der Durchsetzung nationaler Egoismen sinnvolle europäische Lösungen sabotieren. Angesichts der globalen Herausforderung sind zumindest europäische Lösungen nötig; nationale Maßnahmen greifen nicht mehr.

Meinungskontrolle?

Schon seit Jahren ein Problem, seit etwa einem Jahr als solches erkannt, ist die ungezügelte Meinungsmache im Internet, die unter den Stichworten Fake-News und Hass-Posts diskutiert wird. Dass es dazu kommen konnte, liegt weniger an fehlenden technik- und praxiskonformen Gesetzen, sondern am fehlenden Gesetzesvollzug. So verstieß z. B. die personalisierte Werbekampagne der Firma Cambridge Analytica zum Brexit unzweifelhaft gegen europäisches Datenschutzrecht. Oft entspricht das Datenschutzbewusstsein derer, die das Recht durchsetzen müssen, leider nicht den

normativen Anforderungen – nicht nur in Großbritannien. Jedenfalls wären die im US-Präsidentschaftswahlkampf praktizierten Kampagnen personalisierter Ansprache in Europa absolut unzulässig.

Fake-News und Hass-Posts werden heute noch weitgehend nicht durch künstliche Meinungsmachmaschinen produziert, sondern allenfalls hierüber weiterverbreitet. Produziert werden diese „Nachrichten“ vorwiegend von Menschen, die zur Verantwortung gezogen werden müssten und könnten. Dass dies nicht passiert, hat viele Gründe. Der wohl zentrale Grund liegt darin, dass die Verbreitungsportale, die – auch rechtlich – eine Mitverantwortung für die Inhalte haben, diese Verantwortung nicht oder nur zögerlich anerkennen. Die Politik wiederum möchte sich nicht mit den IT-Unternehmen anlegen und setzte lange Zeit auf Selbstregulierung. Diese kann und konnte aber nicht funktionieren, weil eine funktionierende Selbstregulierung eine Beeinträchtigung von deren Geschäft zur Folge hätte.

Die falscheste Reaktion auf diese Entwicklung wäre Zensur oder eine staatliche Einmischung in den demokratischen Diskurs. Derartiges kennen wir in Form einer 50-Cent-Armee in China. Die Unabhängigkeit einer freien Presse ist der beste Garant dafür, dass sich Wahrheiten durchsetzen. Auch eine deutsche Regierung und deutsche Behörden sind nicht davor gefeit, Fake-News zu verbreiten. Und je mehr Behörden über die Menschen wissen, umso leichter können sie diese manipulieren. Dazu liefert China mit seinem Citizen-Score, der gemeinsam mit führenden lokalen Internetfirmen die Systemkonformität jedes einzelnen Menschen berechnet, abschreckendes Anschauungsmaterial.

Internet-Portale sind keine Presseunternehmen und genießen nicht deren Privilegien. Es handelt es sich dabei aber auch nicht um neutrale Verbreitungsinstrumente von Meinungen, die keine Verantwortung für die Inhalte und deren Wirkung hätten. Das Telemediengesetz kennt den Grundsatz des „notice and take down“, also der Verpflichtung, bei entsprechenden Hinweisen Inhalte zu überprüfen und bei Rechtswidrigkeit zu sperren. Die Praxis von Facebook, diese Prüfung an ein billiges Dienstleistungsteam zu delegieren, das unter unwürdigen Bedingungen und nach geheim gehaltenen, mit dem deutschen Recht nicht kompatiblen Kriterien vorgeht, genügt diesen Anforderungen nicht im Ansatz. Tatsächlich haben die sozialen Netzwerke nicht nur eine medienrechtliche Verantwortung, sondern auch eine Garantenstellung und damit eine strafrechtliche Verantwortung, wenn sie auf über ihre Kanäle begangene Straftaten nicht reagieren. Dabei handelt es sich i. d. R. um Beihilfe, in manchen Fällen aber gar um Mittäterschaft.

Es geht natürlich nicht an, Privatfirmen – um solche handelt es sich bei sozialen Medien – zu Wächtern über die freie Meinungsäußerung oder zu Zensoren zu machen. Die Grenze liegt aber dort, wo über diese strafbare Inhalte transportiert werden.

Andere Instrumente als das Strafrecht sind gefordert, wenn wir mit dem demokratischen Meinungskampf im Netz zu tun haben. Hier fehlen uns tatsächlich noch Instrumente und Prozesse, da das Presserecht insofern nicht greift. Dennoch können dort Anleihen gemacht werden. Da Computer keine Meinungsfreiheit für sich beanspruchen können, ist

es von Internetdiensten nicht zu viel verlangt, eine technische Bot-Kontrolle in ihren Netzwerken vorzunehmen. Auch das Reposten von unzulässigen Nachrichten kann technisch minimiert werden. Gegen Falschmeldungen und Persönlichkeitsverletzungen könnte ein vereinfachtes Verfahren der presserechtlichen Gegendarstellung eingeführt werden, das die Anbieter nicht zur Sperrung, wohl aber zur Darstellung korrigierter Fakten verpflichtet.

Ein wichtiges Instrument gegen Fake-News von Politik und Wirtschaftsunternehmen sind Whistleblower. Kurz vor seinem Amtswechsel hat der US-Präsident Barack Obama mit der Begnadigung von Chealsea Manning indirekt ein Zeichen dafür gesetzt, dass das Offenlegen unmenschlicher US-Militärpolitik durch „Verrat von Staatsgeheimnissen“ einen wichtigen Beitrag für unseren demokratischen Diskurs dargestellt hat. Diese Begnadigung ist aber kein Indiz für einen Richtungswechsel beim Umgang mit Whistleblower. Edward Snowden steht in den USA weiterhin auf der Liste der „most-wanted-persons“. Strukturell und rechtlich ist Whistleblowing insbesondere auch in Deutschland bis heute nicht anerkannt. Das muss sich ändern

Demokratie 4.0

Demokratie ist in ihren griechischen Ursprüngen mehr als 2000 Jahre alt. Unsere moderne Demokratie mit gleichem Wahlrecht und Meinungsfreiheit ist weniger als 200 Jahre alt und musste und konnte sich – bis heute – immer weiter entwickeln und ausdifferenzieren. Es ist offensichtlich, dass die Informationstechnik neue Rahmenbedingungen schafft, auf die mit angepassten technischen, organisatorischen rechtlichen Regeln reagiert werden muss. Inakzeptabel ist es, unsere Freiheitsrechte abzuschalten, so wie dies derzeit in der Türkei, in Ägypten und in vielen anderen Staaten passiert. Vielmehr müssen wir unsere Freiheitsrechte digital fortschreiben. Auch wenn dabei nicht schon der Stein des Weißen gefunden wurde, ist deshalb die „Charta der digitalen Grundrechte“, die nachher mein früherer Kollege Johannes Caspar vorstellen wird, der richtige Ansatz. Nicht akzeptabel ist dagegen die bisherige Praxis unserer Bundesregierung, der zwar „Industrie 4.0“ leicht über die Lippen geht, die aber keine Idee von „Demokratie 4.0“ hat. Wir können und wir sollten ihr dabei auf die Sprünge helfen.