Wirtschaft 4.0 und die Wertentscheidung für den Datenschutz

Ein Zwischenruf

Der vorliegende Text ist eine überarbeitete Fassung eines Vortrags von Thilo Weichert auf der 39. DAFTA am 19.11.2015 in Köln.

Stand: 31.12.2015

Inhalt

Thilo Weichert
Waisenhofstr. 41
0431 9719742
weichert@netzwerk-datenschutzexpertise.de
www.netzwerk-datenschutzexpertise.de

Angesichts der wirtschaftlichen Möglichkeiten moderner Informationstechnik fordern viele Politiker und Wirtschaftsvertreter die Zurückdrängung des Datenschutzes. Der Zwischenruf wendet sich gegen das damit verbundene „Primat der Wirtschaft“ und plädiert für ein „Primat des Rechts“.

1 Informationswirtschaft

Für die Bezeichnung der technisch bedingten Struktur-Transformation unseres Lebens und Wirtschaftens wird gerne der Begriff „Informationsgesellschaft“ verwendet. Diese löst nicht die sich im 19. und 20. Jahrhundert entfaltende Industriegesellschaft ab, sondern ergänzt sie um die Dienstleistungs- und schließlich sehr umfassend um die Digitalisierungskomponente. Rohstoffbasierte Massenproduktion und Automation werden nicht abgelöst, sondern weiterentwickelt. Mit Begriffen wie „Industrie 4.0“ oder „Wirtschaft 4.0“ werden die überwiegend digital gesteuerten Produktionen und Dienstleistungen bezeichnet – unter Einsatz von „Smart Factory“ und „Big Data“, zwei weiteren Schlagworten, die bestimmte, hochdigitalisierte Nutzungen bezeichnen – von der Industrieproduktion über den Verkehr, bis hin zum Gesundheits- und Bildungssystem.

Es ist erst wenige Jahre her, dass diese Begriffe in der Politik angekommen sind, verbunden mit der Verheißung, dass der Industrieweltmeister Deutschland zumindest im Bereich der Warenproduktion den Angriff des unbestrittenen Informationsweltmeisters USA abwehren könne. Derweil bauen die USA, wo die Digitalisierung auf Massenbasis schon vor mehr als 10 Jahren angekommen ist, ihre Weltmeisterschaft im Kommunikations- und im IKT-Konsumbereich weiter aus. Die deutsche Politik hat zwar die wirtschaftliche Bedeutung der Digitalisierung erkannt und pilgert nun ins Silicon Valley im sonnigen US-amerikanischen Kalifornien, hat aber noch nicht ansatzweise analysiert, geschweige denn verstanden, mit welchen Wertherausforderungen die Informationswirtschaft dabei konfrontiert wird.

Ein zentrales Merkmal unserer Informationsgesellschaft besteht darin, dass Information zur Ware und zum Produktionsfaktor wurde. Diese Entwicklung hat schon vor Jahrzehnten eingesetzt und spätestens mit dem Beginn des Jahrhunderts alle Wirtschaftsbereiche erfasst. Unser Rechtssystem hat darauf reagiert, indem es sogenannte immaterielle, informationelle Rechte schuf, so schon früh das Urheberrecht und die aus dem Eigentumsrecht abgeleiteten Betriebs- und Geschäftsgeheimnisse. Seit den 70er Jahren des vergangenen Jahrhunderts entwickelte sich vor diesem Hintergrund aus dem allgemeinen Persönlichkeitsrecht der Datenschutz, dem seit 2009 europaweit normativ abgesichert, Grundrechtsstatus zukommt. Während aber die vermögensrechtliche Relevanz von Urheberrechten und Geschäftsgeheimnissen von Anfang an anerkannt war, tun sich Gesetzgebung und Rechtsprechung bis hin zur Steuerverwaltung bis heute schwer, diesen Schritt auch für personenbezogene Daten zu vollziehen. Dies gilt insbesondere für Kundendaten, deren vermögensrechtliche Seite vom Gesetzgeber weiter ignoriert wird, wenngleich das Vermögen großer Internetunternehmen – teilweise fast ausschließlich – auf ihrem detaillierten Wissen über ihre Kunden basiert.

2 Technische Entwicklungen

Die augenblickliche Entwicklung bei der Digitalisierung der Wirtschaft ist durch den Gebrauch von Begriffen wie „mobile“, „social“, „cloud“ und „analytics“ gekennzeichnet. Durch die rasante

Weiterentwicklung der Funktechnologie und die Miniaturisierung von Endgeräten sind Datenverarbeitung und Kommunikation nicht mehr an feste Standorte gebunden. Der Einsatz so genannter sozialer Medien hat zu einer quantitativen Intensivierung und zugleich qualitativen Banalisierung der elektronischen Kommunikation geführt wie auch zur Auflösung bisher klar getrennter gesellschaftlicher Rollen, insbesondere zur Aufhebung der Trennung zwischen Privat- und Arbeitsleben. Die Datenverarbeitung erfolgt physikalisch nicht mehr zwangsläufig auf eigenen und eigenkontrollierten Rechnersystemen, sondern zunehmend bei mehr oder weniger anonymen Dritten in der Cloud oder auf formal eigenen, jedoch mit fremdkontrollierter Software betriebenen Rechnern. Die so verarbeiteten, in großen Mengen anfallenden Daten werden, soweit dies die jeweiligen Rechtsordnungen nicht wirksam verbieten, umfassenden Analysen unterworfen. Diese dienen unterschiedlichsten Zwecken, im Bereich der Privatwirtschaft insbesondere der Erzielung eines zusätzlichen ökonomischen Mehrwertes.

Diese Entwicklung wurde technisch durch die fast unbegrenzte Erhebungs-, Speicherungs- und Auswertungskapazität moderner Datenverarbeitung möglich. Fortschrittstrunken wird von Politik und Wirtschaft „Big Data“ gehuldigt, dem unspezifischen Schlagwort, das nach verbreiteten Definitionsversuchen zumindest dreierlei Charakteristika bei der Datenverarbeitung aufweist: Volume, Variety und Velocity. Quantitativ extrem große Datenmengen werden trotz der Vielfalt der Formate und Kontexte und weitgehend ungeachtet bestehender rechtlicher Bindungen zusammengeführt und in kurzer Zeit, evtl. gar in Echtzeit, analysiert und so als Grundlage für unterschiedlichste Entscheidungen verwendet. In vielen Fällen wird eine so herbeigeführte Entscheidung über nicht ganz unwesentliche Dinge, etwa über den Abschluss von Verträgen, durch einen vollständig automatisierten Algorithmus getroffen. Im klassischen Industriebereich erfolgen so Produktionsentscheidungen. Hier und in anderen Lebensbereichen, etwa beim Konsum, aber selbst bei der politischen Planung, werden Entscheidungen getroffen, die Menschen betreffen. So wird per Computer festgelegt, wer unter welchen Voraussetzungen einen Kredit[1], ein Warenangebot oder eine Arbeitsstelle bekommt. Noch nicht vorgegeben, aber durch die Festlegung gezielter Werbemaßnahmen wesentlich vom Computer mitbestimmt wird z. B., wer in den USA Präsident wird.[2]

Aus persönlichkeitsrechtlicher Sicht sind die Schnittstellen zwischen den IT-Systemen und den Menschen von besonderem Interesse. Die Zeiten, in denen die analoge Welt des Menschen von der digitalen Welt kleiner und großer Netzwerke getrennt war, sind vorbei. Die Verbindung des Menschen zum Computer sind nicht mehr nur Tastatur, Bildschirm und Drucker, sondern Sprache, Mimik und Gesten. Der Mensch wird zunehmend integraler Bestandteil informations- und kommunikationstechnischer (IKT-) Systeme. Die klassischen – drahtlosen – Verbindungen zwischen Mensch und System sind personifizierte IT-Endgeräte, also PC, Tablet und Smartphone, privat und am Arbeitsplatz, zunehmend auch stationär über Smart Home oder Smart City und mobil etwa über Wearables oder Connected Cars. Am vollständig automatisierten Arbeitsplatz wird das nachgeholt, was die Fließbandarbeit vor 100 Jahren noch nicht schaffte: Der Beschäftigte wird digital in den

[1] Inwieweit dies bei ungenügender Transparenz für die Betroffenen verfassungskonform ist, wird derzeit im Rahmen einer Verfassungsbeschwerde gegen die Entscheidung des BGH v. 28.01.2014, VI ZR 156/13, durch das BVerfG geprüft.

[2] Wir sind Algorithmus-Zombies, http://www.taz.de/!5243063/.

Produktionsprozess integriert, im schlechtesten Fall als menschlicher Ausputzer maschinell noch nicht beherrschbarer Prozesse, im besseren Fall als Kontrolleur und Pannenhilfe. Art und Geschwindigkeit der Produktion werden automatisiert berechnet und vorgegeben. Selbstbestimmung ist dabei kaum oder gar nicht mehr möglich. Als digitale Hilfsmittel kommen zunehmend Virtualisierungsinstrumente wie z. B. Smart Glasses zum Einsatz, mit denen die Wahrnehmungsfähigkeit des Menschen ebenso gesteigert werden kann wie auch die Kontrolle seines Verhaltens und seiner Leistung.[3]

Die Weiterentwicklung ist vorgezeichnet: Die Mensch-Maschine-Schnittstelle wird noch näher an oder in den Menschen gebracht, etwa durch biotechnische Sensorik, digitale Implantate oder körperlich-digitale Erweiterungen. Der Mensch wird bei vielen Aktivitäten durch Roboter ersetzt. So feiert z. B. ein Baby-Betreuungs-Roboter Markterfolge, der wie von Geisterhand die Armbewegungen von Eltern, aber auch Autofahrten oder Wasserwellen simuliert. Die eingebaute Sensorik erkennt und stillt umgehend die Bedürfniswechsel des Babys.[4]

Die Integration von Bio- und Informationstechnik steckt noch in den Kinderschuhen. Medizinische Sensoren unterstützen medizinische Diagnosen und Therapien und ermöglichen gesundheitliche Dauerüberwachungen oder auch die ärztliche Fernbetreuung. Ein möglicher Anwendungsfall ist das Ambient Assisted Living (AAL) hilfsbedürftiger Personen.[5] Noch spannender wird es, wenn die genetische Sensorik und Analytik weiterentwickelt werden. Derzeit erlauben solche Anwendungen noch keine Echtzeitreaktionen. Doch etabliert sich die Genanalyse nicht nur im klassischen medizinischen Behandlungs- und Forschungsbereich, sondern auch auf anderen Feldern wie Lifestyle und Wellness, am Arbeitsplatz oder im Versicherungsmarkt. Dabei folgt auf die Analyse die Manipulation, bzw. freundlicher ausgedrückt: die genetische Gestaltung. Genome Editing findet derzeit – auch bei Menschen – erste Anwendungen.[6]

3 Triebfedern des digitalen Wandels

Ursache all dieser Veränderungen ist nicht zuletzt der menschliche Forschungsdrang. Eine weitere Triebfeder mögen staatliche Kontroll- und Überwachungsbedürfnisse sein. Das Hauptversprechen der Digitalisierung ist aber ein Ökonomisches. Es geht um Kosteneinsparungen und um das Erzielen zusätzlicher Profite. Angesichts des globalen Wettbewerbs besteht dauernder Entwicklungsdruck. Die wissenschaftlichen Fortschritte in der Informations- und Biotechnik werden weniger von ethischem oder aufklärerischem Bestreben getrieben als davon, die eigene Marktmacht auszudehnen. In diesem Sinne erscheint Big Data als Heilsbringer, zum Beispiel durch Effizienzsteigerungen im Bereich der Planung und der Organisation oder durch automatisierte Entscheidungen, die Menschen selektieren,

[3] Bernhardt, Google Glass: On the implications of an advanced military command and control system for civil society, http://www.i-r-i-e.net/inhalt/020/IRIE-Bernhardt.pdf.

[4] Werner, Schlaf, Kindlein schlaf, der Roboter hüt´ die Schaf, SZ 11.11.2015, 26.

[5] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Juristische Fragen im Bereich Altersgerechter Assistenzsysteme, https://www.datenschutzzentrum.de/uploads/projekte/aal/2011-ULD-JuristischeFragenAltersgerechteAssistenzsysteme.pdf.

[6] Grolle, Menschen nach Maß, Der Spiegel 49/2015, 125 ff.

manipulieren und diskriminieren. Personalisierung mittels Big-Data-Anwendungen bezieht sich nicht nur auf die Werbung, sondern hat über Bonitätsbewertungen und Konsumanalysen schon längst die Vertragskonditionen und die Preise erfasst. Heute darf der Apple-Kunde auf Hotelsuche gerne etwas mehr bezahlen, kann er sich doch ein teures Endgerät leisten und gehört vermutlich einer bessergestellten Zielgruppe an. Haupt-Zielgruppe der digitalen Übervorteilung ist heute kaum mehr die unbedachte ältere Oma, der per Cold Call ein Zeitschriftenabo untergeschoben wird. Der Fokus liegt auf dem Durchschnittsuser und insbesondere bei den mit digitalen Gadgets aufgewachsenen Jugendlichen, denen spielerisch-konsumierend das Geld aus der Tasche gezogen wird.

Wirtschaft 4.0 und Industrie 4.0 versprechen Goldgruben zu werden. Fatal an diesen Gruben ist, dass, wer sich – als Unternehmer wie auch als Konsument – nicht auf sie einlässt, in eine andere Grube zu stürzen droht: Wer nicht im großen Spiel mitspielen will und keine Nischen findet, dem droht der ökonomische und gesellschaftliche Absturz, in jedem Fall aber, vom globalen Markt abgehängt zu werden.

4 Falsche Wertsetzungen

Welche Konsequenzen hat dies für unsere gesellschaftlichen Werte? Bisher sucht man in Deutschland mit den Begriffen „Wirtschaft 4.0“ und „Industrie 4.0“ den Anschluss an den Silicon-Valley-Kapitalismus. Dieser unterscheidet sich vom Manchester-Kapitalismus des 19. Jahrhunderts dadurch, dass er weniger zur materiellen Verarmung des Proletariats führt, sondern eher zu geistiger Verarmung, verbunden mit einem Konsumangebot, das diese Verarmung für viele erträglich macht. Compliance, also Konformität mit rechtlichen und ethischen Regeln, streben die großen Player nur an, solange durch die Einhaltung der Regeln keine Einbußen bei Marktchancen und Profit oder wenn damit im Wettbewerb verwertbare Alleinstellungsmerkmale verbunden sind. Diese Haltung entwickelt sich bisher unter den wohlwollenden Augen der Politik. So forderte Bundeskanzlerin Angela Merkel die deutsche Bevölkerung auf, endlich ihre ständigen Datenschutz-Bedenken fallen zu lassen und den Schutz ihrer Privatsphäre der Entwicklung der nationalen Wirtschaft unterzuordnen, um im digitalen Zeitalter international mithalten zu können.[7] Verblüffend ist nur auf den ersten Blick, dass sich insbesondere die CDU/CSU, die noch kürzlich eine deutschen Leitkultur propagierte, sich als Fürsprecher des US-amerikanischen Vorbildes profiliert und dabei nicht nur die bürgerrechtlichen und demokratischen, sondern auch die globalen sozialen Kosten ausblendet. Entsprechend einsilbig waren die politischen Reaktionen auf die Safe-Harbor-Entscheidung des Europäischen Gerichtshofs vom Oktober 2015.[8] Dieses Urteil kann kurz und knapp damit auf den Punkt gebracht werden, dass Grundrechtsschutz und dessen Durchsetzung – anders als bisher die Praxis – durch unabhängige Aufsichtsbehörden und Gerichte absolute Priorität vor Interessen von Wirtschaft und Industrie haben müssen.

Dem setzt die Politik das „Primat des ökonomischen Erfolgs“ entgegen. Sie ignoriert dabei, dass eine große ökonomische Chance für die europäische Wirtschaft in der Entwicklung einer werteorientierten, transparenten und demokratisch kontrollierten Informationswirtschaft liegt. Wer sich die

[7] Merkel gegen zu viel Datenschutz, DANA 4/2015, 176.

[8] EuGH, Urteil v. 06.10.2015, C-362/14.

gesellschaftlichen Alternativen großer IT-Nationen wie die USA oder China vor Augen führt, müsste eigentlich die Alternativlosigkeit des europäischen, vom EuGH vorgegebenen Wegs für eine freiheitliche demokratische Gesellschaft erkennen. Die vorherrschenden Menschenbilder und die gesellschaftlichen und kulturellen Strukturen der anderen wichtigen IKT-Wirtschaftssysteme sind mit unserer Verfassungskultur nicht vereinbar: Da ist einerseits der US-amerikanische Exzeptionalismus, der seine militärische und informationstechnische Dominanz nutzt, nicht nur um andere Staaten informationell auszubeuten, sondern auch um sie zu beherrschen. Edward Snowden verdanken wir insofern einige aufschlussreiche Einsichten. Gar nicht zu reden – andererseits – vom chinesischen Kollektivismus, der durch informationelle Kontrolle, Manipulation und durch digitale Konsumangebote seine Milliardenbevölkerung ruhigzustellen versucht und so zugleich die autoritäre Herrschaft einer kleinen Parteiclique absichert. Auch der russische Paternalismus, für den das ökonomische Wohl einer kleinen oligarchischen Schicht im Vordergrund steht, sollte für uns keine Alternative sein.

5 Datenschutz als informationelles Rundum-Grundrecht

Im globalen Wertestreit hat der Datenschutz eine zentrale Bedeutung. Die vom Bundesverfassungsgericht in einer Vielzahl von Entscheidungen entwickelten, aus unserer Verfassung und unseren Grundrechten abgeleiteten Werte wurden inzwischen vom Europäischen Gerichtshof in seinen Urteilen zur TK-Vorratsdatenspeicherung[9], zu Google Search[10] und zu Safe Harbor[11] bekräftigt und in ihrer europaweiten Gültigkeit bestätigt. Danach gelten die Grundrechte als individuelle wie auch gesellschaftlich-institutionelle Garantien nicht nur gemäß ihrem überkommenen analogen Verständnis, sondern auch im virtuellen digitalen Raum. Durch das Verbot personenbezogener Datenverarbeitung mit gesetzlichem Erlaubnisvorbehalt gilt nicht das Primat des Profits, sondern das der demokratischen Entscheidung, deren Werthaltigkeit von unabhängigen Datenschutzbehörden kontrolliert und von Gerichten rechtsstaatlich sichergestellt wird. Letztlich werden durch die digitalen Grundrechte auch sozialstaatliche Fragen beantwortet, wie der Staat angesichts der Herausforderungen digitalen Wirtschaftens Empathie und Fürsorge für die Nichtprivilegierten sicherstellen soll. Verboten sind nicht nur informationelle Diskriminierungen wegen Geschlecht, Ethnie oder sexueller Orientierung. Auch die Ungleichbehandlung auf der Basis sozialer Kriterien bedarf einer gesetzlichen Rechtfertigung.

Die Rechtswissenschaft hingegen blieb im großen Ganzen phänomenologisch. Sie hat trotz der überzeugenden Argumentation des Bundesverfassungsgerichts die Bedeutung und Brisanz des Grundrechts auf informationelle Selbstbestimmung nicht umfassend erfasst und gewürdigt. Dieses Grundrecht hat eben nicht nur eine individualrechtliche, den Staat abwehrende Dimension. Ihm kommt vielmehr auch eine ordnungsrechtliche Dimension zu, die unsere Art des Wirtschaftens bestimmt. Das Recht schützt explizit vor informationeller Fremdbestimmung und Ausbeutung durch den ökonomisch und informationell Stärkeren. Wer etwa die Entscheidung zur Schweigepflichtentbindung in Versicherungsverhältnissen liest, erkennt darin eine Absage an den

[9] EuGH, U. v. 08.04.2014, C-293/12 u. C-594/12.

[10] EuGH, U. v. 13.05.2014, C-131/12.

[11] EuGH, U. v. 06.10.2015, C-362/14.

gelebten Silicon-Valley-Kapitalismus.[12] Informationelle Selbstbestimmung bedeutet auch informationelles Diskriminierungsverbot. Der Datenschutz hat eine materielle soziale Dimension. Und nicht nur das. In vielen Urteilen stellt das Bundesverfassungsgericht – zur Volkszählung[13], zur Brokdorf-Demonstration[14] , zur TK-Vorratsdatenspeicherung[15] – die Bedeutung des Datenschutzes als informationelle Voraussetzung für die demokratische Teilhabe heraus. In der Safe-Harbor-Entscheidung hat der EuGH zudem betont, dass das Grundrecht auf Datenschutz ein effektiv durchsetzbares Recht sein muss. In Europa soll die Herrschaft des Rechts, der Rule of Law, gelten, nicht die Herrschaft von Wirtschaftsunternehmen.[16]

Die materiellrechtliche Wertentscheidung für den Datenschutz wird operationalisiert durch die technisch-organisatorischen Schutzziele der Verfügbarkeit, Integrität, Vertraulichkeit, der Transparenz, Intervenierbarkeit und Nichtverkettbarkeit bei der Datenverarbeitung.[17] Diese Schutzziele dienen also nicht der Abwehr einzelner separierbarer Risiken, sondern der Wahrung von Demokratie, Freiheitlichkeit, Sozial- und Rechtsstaatlichkeit unserer Informationsgesellschaft und unseres digitalen Wirtschaftens, individuell und gesamtgesellschaftlich.

6 Auf dem Weg zu digitaler Souveränität

Sämtliche der oben beschriebenen Schutzziele lassen sich nur verwirklichen, wenn wir unsere digitale Souveränität wahren. Insofern ist die Realität bedrohlicher, als wir uns bisher eingestehen: Digital souverän, d. h. umfassend entscheidungsmächtig über die uns betreffenden digitalen Fragen, sind wir in der Praxis auf keiner Ebene. Die Beherrschbarkeit der von uns verwendeten IKT-Systeme wäre Voraussetzung für unsere individuelle wie auch für unsere gesellschaftliche demokratische Selbstbestimmung. Nur wenn wir wüssten, was die von uns verwendete IKT bewirken kann und auch tatsächlich bewirkt, könnten wir für deren Resultate voll die Verantwortung übernehmen.

Dieser eigentlich selbstverständliche Ansatz hat mit der Wirklichkeit wenig zu tun. Seit Jahren verlassen wir uns auf die Software-Aktualisierungen unserer – zumeist US-amerikanischen – Systemanbieter. Spielten wir die Updates zunächst noch separat auf die von uns verwendeten Rechner, so passiert dies inzwischen meist im Hintergrund, ohne dass wir hiervon überhaupt noch Notiz nehmen. Wir liefern uns erst recht anonymen Dienstleistern aus, wenn wir deren Cloudangebote nutzen. Welche Konsequenzen dies hat, führte uns Edward Snowden vor Augen, der dargelegte, das ein großer Bruder vor allem über die Zwischenschaltung vieler Netz- und Dienstebetreiber alles mitlesen kann. Digitale Souveränität ist aber nicht nur Voraussetzung zur Vermeidung des

[12] BVerfG, B. v. 23.10.2006, JZ 2006, 576 ff., vgl. BVerfG, B. v. 17.07.2013, JZ 2013, 1156 ff.

[13] BVerfG, U. v. 15.12.1983, NJW 2014, 419 ff.

[14] BVerfG, B. v. 14.05.1985, EuGRZ 1985, 450 ff.

[15] BVerfG, U. v. 02.03.2010, NJW 2010, 833 ff.

[16] EuGH, U. v. 06.10.2015, C-362/14, Rn. 95.

[17] Rost, Die Schutzziele des Datenschutzes, in: Schmidt/Weichert, Datenschutz, 2012, S. 353 ff.

Ausgespähtwerdens. Ohne sie sind wir selbst auch nicht in der Lage, aktive Eingriffe und Manipulationen unserer IKT durch Dritte abzuwehren.[18]

Was schon für Privatnutzende heikel ist, wird für Wirtschaftsunternehmen absolut unakzeptabel. Diese haben eine rechtliche und soziale Verantwortung für ihre Beschäftigten und ihre Kunden sowie vor der Gesellschaft, die von ihnen verantworteten Daten angemessen und nachvollziehbar zu schützen. Tatsächlich liefern sich jedoch viele Unternehmen – oft ohne vertragliche Rückversicherung – Software- und Clouddienstleistern aus und verlieren so jede Möglichkeit, ihren Pflichten kontrollierbar nachzukommen. Geködert werden Unternehmen mit scheinbar niedrigen Betriebs- und Lizenz-Kosten und der Fiktion einer kostengünstigen Administration durch den Cloudanbieter, wie etwa für Office 365 oder Windows10. Die Hoffnung, dass der Markt die Dienstleister disziplinieren würde, ist schon wegen der Marktdominanz einzelner Unternehmen Selbstbetrug.

Wir wissen nicht und können nicht wissen, welche Hintertüren in der von uns genutzten Informationstechnik steckt und wie wir uns gegen Angriffe durch Dritte zur Wehr setzen können. Dies kann desaströse Wirkungen auslösen: Stuxnet scheint sich vor allem gegen den Iran gerichtet zu haben.[19] Regins Unwesen können wir bisher nicht ansatzweise abschätzen.[20] Welchen Angriffen unsere IKT-Systeme ausgesetzt sind, bekommen wir oft gar nicht mit. Zur digitalen Souveränität gehört nicht nur die Kontrolle über die eigene IKT, sondern auch die demokratische Kontrolle über unsere IKT-Sicherheitsinfrastruktur.

Eine weitere Drehung in der Spirale der organisierten Verantwortungslosigkeit stellt das Bauen auf sogenannte „künstliche Intelligenz“ dar. Überlassen wir Computern Entscheidungen, die auf selbstlernenden (und daher veränderlichen), möglicherweise nicht mehr dokumentierten und nachvollziehbaren Algorithmen basieren, so haben wir das Heft völlig aus der Hand gegeben.[21] Der Börsencrash 2008 wurde dadurch verstärkt, dass die Computer der Aktienhandelsplätze Amok liefen.[22] Es gibt noch kritischere Infrastrukturen als unsere Finanzsysteme, etwa wenn es um unsere Wasser- oder Energieversorgung geht.[23]

7 Schlussfolgerungen

Was bedeutet das für Wirtschaft und Industrie 4.0? Wir müssen uns unsere Souveränität im digitalen Raum erst erobern. Dafür ist digitale Kompetenzvermittlung grundlegend. Dies gilt für uns als Nutzer und für Führungskräfte in Wirtschaft und Industrie. Dies gilt vor allem aber für die Politik, die weiterhin

[18] Greenwald, Die globale Überwachung, 2014.

[19] http://www.heise.de/thema/Stuxnet.

[20] Wölbert, Zweites Ermittlungsverfahren wegen NSA-Spionage in Deutschland, www.heise.de 25.10.2015.

[21] Helbing/Frey/Gigerenzer/Hafen/Hagener/Hofstetter/van den Hoven/ Zicari/Zwitter, Das Digital Manifest, 12.11.2015, www.spektrum.de.

[22] Hofstetter, Sie wissen alles, 2014, S. 97 ff., 151 ff.

[23] Eindringlich Elsberg, Blackout, 2012.

unbekümmert und ohne ausreichende Kompetenz auf dem Vulkan tanzt. Es darf keine Geschäfts- und keine Staatsgeheimnisse geben, wenn vitale Fragen der digitalen Souveränität, also die individuelle und die demokratische Kontrolle der Sicherheit und der Intervenierbarkeit unserer Datenverarbeitung, betroffen sind. Open Source kann eine adäquate Antwort sein. Wichtig ist die transparente Standardisierung von IKT. Bis heute werden Standards in der IKT vor allem marktgesteuert entwickelt. Allgemein gültige Normen, die unsere Datenverarbeitung bestimmen, müssen diskutiert und überprüft werden können. So selbstverständlich wir demokratisch diskutierte und beschlossene Regeln im Straßenverkehr kennen, benötigen wir diese auch im Datenverkehr. Es genügt nicht, marktgängige Zertifizierungen einzuführen, wie wir sie im Bereich der IT-Sicherheit ansatzweise kennen. Im Bereich des Datenschutzes sind diese Zertifizierungen auch 15 Jahre, nachdem sie in Schleswig-Holstein entwickelt wurden[24], immer noch nicht etabliert. Die Verantwortlichkeit der Produkthersteller und -anbieter hat sich bis heute im Datenschutz nicht durchgesetzt.

Bei aller Begeisterung für das Digitale muss außerdem regelmäßig geprüft werden, inwieweit für digitale Lösungen analoge Alternativen bewahrt werden müssen. Dies gilt nicht nur für den Bezahlprozess durch die Bewahrung des anonymen Bargeldes, sondern auch für Wahlen, die Postzustellung und andere grundlegende Prozesse, z. B. im Bereich politischer und ökonomischer Entscheidungsfindungen.[25]

Zudem benötigen wir eine Infrastruktursicherung, die sich nicht – wie das soeben verabschiedete IT-Sicherheitsgesetz – auf reine Sicherheit, kritische Infrastrukturen und unverbindliche Vorgaben beschränkt.[26] In einer umfassenden Netzinfrastruktur sind verbindliche Datenschutzvorgaben erforderlich, die technisch und organisatorisch, und wenn nicht anders möglich, durch Verbots- und Gebotsregelungen umgesetzt werden. Bei der Festlegung unseres Regelungsrahmens sind neben materiell-rechtlichen Regelungen zunehmend zusätzliche prozessuale Sicherungen vorzusehen, um die prozesshafte Weiterentwicklung unserer IKT adäquat begleiten zu können.

Ein weiterer erfolgversprechender Ansatzpunkt für eine effektive Regulierung unserer digitalisierten Wirtschaft kann in der Einbeziehung verbandlicher Interessenwahrnehmung der Betroffenen liegen. Ein winziger Schritt in diese richtige Richtung wäre die Einführung eines Klagerechts von Verbraucherverbänden bei Datenschutzverstößen, die schon seit Monaten verzögert wird.[27] Die Europäische Datenschutz-Grundverordnung kann insofern mit ihrem Artikel 76 weiteren frischen Wind bringen. Völlig unbearbeitet blieb dabei bisher der Beschäftigtendatenschutz. Die Betroffenenvertretungen, also Betriebsrat und Gewerkschaften, sollten mit Mitentscheidungs- und Klagerechten ausgestattet werden, um sie betreffende digitale Verfahren mitgestalten zu können.

---

[24] ULD, https://www.datenschutzzentrum.de/guetesiegel/.

[25] Aufschlussreich insofern BVerfG, U. v. 03.03.2009, DVBl 2009, 511 ff. zur Verwendung von Wahlcomputern.

[26] Bernhardt/Ruhmann, IT-Sicherheit nach dem neuen IT-Sicherheitsgesetz, 2015, https://www.datenschutzzentrum.de/uploads/sommerakademie/2015/SAK2015_02-Vormittag_BernhardtRuhmann_IT-Sicherheitsgesetz_Handout.pdf.

[27] Stöcker, Interview mit Müller, „Da hängen wir gerade“, www.spiegel.de 24.09.2015.

Bei aller begründeten Kritik an der aktuellen IKT-Politik der USA: Angesichts der noch bestehenden Dominanz der US-amerikanischen Anbieter und der Herausforderungen durch völlig andere gesellschaftliche und ökonomische Kulturen, etwa aus Südostasien, sollten sich Nordamerika und Europa auf ihre gemeinsamen demokratischen und freiheitlichen Werte besinnen und diese im digitalen Raum umsetzen. Der transatlantische Dialog hierzu ist dringender denn je. Das aktuelle Safe-Harbor-Urteil liefert dafür einen guten Ansatzpunkt. Eine Verständigung mit den USA ist aber nur möglich, wenn Europa einen klaren Standpunkt vertritt und diesen konsequent mit ökonomischem und politischem Druck zur Geltung bringt.

Datenschutz bei Wirtschaft 4.0 ist eine gewaltige Aufgabe und Herausforderung. Wir haben damit erst angefangen.