



Wir begrüßen die behördliche Transparenzinitiative, den Verzicht auf Anstöße zur Ersetzung des Bargeldes, den Verzicht auf neue Behörden-Datensilos im "Big Data"-Stil, den Verzicht auf diskriminierendes "Predictive Policing", den Ausbau neutraler Netze als universell und frei einsetzbares Kommunikationsmittel und zu guter Letzt die Einbindung des ULD in viele Entscheidungen und Prozesse.

Wir vermissen im uns vorliegenden Entwurf die Absage an die Vorratsdatenspeicherung und ein explizites Bekenntnis zum anonym nutzbaren Mobilfunk. Selbstbestimmte Vernetzung muss das oberste Ziel jedes Breitbandausbaus sein: Provider zu verpflichten, auf eigene Kosten ein detailliertes Protokoll des Verhaltens der Anschlussnutzer zu führen, ist eine durch nichts zu rechtfertigende Ungeheuerlichkeit, die dem zuwidersteht. Sie entspringt dem Denken und dem Instrumentarium von Diktaturen. Auch wünschen wir uns ein explizites Bekenntnis zu freier Software<sup>1</sup>, die im Computerzeitalter eine unabdingbare Grundlage für einen selbstbestimmten Umgang mit der umgebenden Informationstechnologie ist.

Wir begrüßen die Verwendung von Informationstechnologie als Werkzeug: dort, wo es sinnvoll ist, mit konkreter Technikfolgenabschätzung und mit einem durch entsprechende Vorgaben gestützten Bewusstsein für die damit verbundene Verantwortung. Allerdings würden wir uns in der Einleitung eine kritische Auseinandersetzung mit den eingeführten Schlagworten und die Nennung weniger bekannter Digitalisierungskonzepte jenseits des Datenkapitalismus und seiner erbarmungslosen Logik wünschen. Hierzu führen wir im Text viele Beispiele und Erklärungen an.

Wir warnen eindringlich vor einer zwangsweisen und überhasteten "Verdatung" aller Vorgänge im Land. Auch warnen wir vor der Unterordnung des Lebens unter Modelle und Technologie. Humanistische Werte müssen die Entwicklung auf jedem Schritt bestimmen. Vernetzung im Alltag darf weder Selbstzweck sein noch irgendjemandem aufgezwungen werden und Effizienz ist nicht das Maß aller Dinge.

Wir sind der Auffassung, dass nicht der Zweck allein über die Sinn- und statthaftigkeit der Digitalisierung entscheidet: bei unserer bisweilen skeptischen Bewertung bestimmter Vorhaben spielt der intendierte Zweck eine untergeordnete Rolle, weil automatische Datenerfassung und -verarbeitung, auch mit den besten Intentionen, stets zu einer gefährlichen Eigendynamik neigen.

---

1 <https://fsfe.org/about/basics/freesoftware.de.html>

Insgesamt hoffen wir, dass unsere Kritik (die sich auf einige Bereiche konzentriert, die unseren Meinungen nach verbessert, besser beleuchtet oder konkretisiert werden sollten) als mahnend, warnend, aber zugleich als konstruktiv verstanden wird - so ist sie gemeint - und einige unserer konkreten Vorschläge es in die nächste Version der in einigen Bereichen durchaus schon ausgereiften digitalen Agenda schaffen.

## **Forderungen, kritische Anmerkungen und Anmahnungen**

Ziel und Zweck der digitalen Agenda muss die Förderung des selbstbestimmten, freien Lebens im Computerzeitalter sein.

Vorbehalte gegen die Digitalisierung aller Lebensbereiche sind keine "Ängste", sondern beruhen auf den bisherigen globalen Erfahrungen im Umgang mit Informationstechnologie. Einerseits bietet die IT neue Möglichkeiten der (Selbst)Organisation, andererseits gerät sie nur all zu leicht zu einem kaum zügelbaren Kontroll-, Überwachungs- und Einengungsinstrument in den Händen staatlicher Stellen wie privater oder gewinnorientiert handelnder Personen, Gruppen oder Unternehmen.

**Komplementär zu Abschnitt 4.2 des Entwurfs fordern wir daher ein Recht auf analoge Teilhabe. Dieses Recht möge in der Landesverfassung verankert werden und muss die Strategie im Umgang mit digitaler Technologie bestimmen. Kein erhoffter Vorteil der Digitalisierung darf das Recht der Menschen auf informationelle Selbstbestimmung oder andere Grundrechte übertrumpfen.**

Die neulich von wichtigen politischen Entscheidungsträgern geäußerte Programmatik, Datenschutz sei als Wachstumshindernis ein Thema von gestern und heute müsse man die Datenindustrie fördern, ist eine Torheit. Diese Torheit - das Wachstum der Datenindustrie und der staatliche Zugriff auf die entstehenden Datenberge - wird unser selbstbestimmtes Leben und die freiheitlich-demokratische Grundordnung auf lange Zeit ruinieren.

Im Gegenteil: Datenschutz - und mindestens genau so wichtig der damit verknüpfte Persönlichkeitsschutz - wird gerade durch neue Möglichkeiten zur Erhebung und Verwertung von Daten, die die intimsten Lebensbereiche betreffen, aktueller als je zuvor. Zwar gibt eine große Bevölkerungsgruppe freiwillig, ohne ausreichend vertieftes Bewußtsein und ohne Gedanken an die Konsequenzen des eigenen Verhaltens in vielen Situationen und Zusammenhängen des persönlichen, alltäglichen Lebens Daten preis. Dies rechtfertigt jedoch niemals, eine Preisgabe auch denen aufzuzwingen, die sich auch über die Nachteile Gedanken machen.

Nicht jeder Mensch ist zu der derzeit damit verknüpften Bedingung der quasi totalen informationellen Fremdbestimmung bereit, ein sogenanntes "Smartphone" zu nutzen. Viele "Zukunftsvisionen" setzen einfach voraus, jeder Mensch müsse irgendwann ein "Smartphone" oder Ähnliches mitführen, weil den Schöpfern dieser Visionen offenbar die Phantasie fehlt, sich ein Leben ohne Datenschatten vorzustellen - für niemanden.

Es gibt aber nun einmal keine Pflicht dazu und so darf es unserer Auffassung nach auch bleiben.

**Daher (auch zu Punkt 2.2.3.):**

**Datensparsamkeit ist die Grundlage jedes wirksamen Datenschutzes, daher muss für persönliche Daten grundsätzlich ein Erhebungsverbot gelten, das Ausnahmen nur aus gewichtigen konkreten Gründen und in engen Grenzen zulässt. Vielmehr möchten wir uns sogar die einstige Aussage von Spiros Simitis zueigen machen: "Demokratie zeichnet sich durch Informationsverzicht aus."**

Ob "die digitale Transformation" gegen diejenigen diskriminieren darf, die nicht jede Kontrolle über ihr Leben freiwillig abgeben wollen, wird damit zu einer Frage des Minderheitenschutzes. Ohne wirksamen Minderheitenschutz aber verkäme die Demokratie zu einer sinnlosen Tyrannei des Stärkeren. Aber auch diejenigen, die eher die Vorteile sehen, würden durchaus von Regulierungen gegen die schlimmsten Auswüchse des Datenkapitalismus, also des ungebremsten Handels mit als "Rohstoff" missverstandenen persönlichen Daten, profitieren.

Bei der im Entwurf eingangs erwähnten "Sharing Economy" geht es um das Teilen - zwischen der Nutzerschaft - mehr aber um das Teilen von Erkenntnissen aus der verdeckten Verhaltensbeobachtung. Diese werden zwangsweise mit einer Entität geteilt, die sich in Geschäftsgeheimnisse hüllt, deren Ziele verborgen bleiben und deren Methoden sich nur bedingt mit einer freien Gesellschaft in Einklang bringen lassen. Die Mitgliedschaft ist nicht offen und kommt für Menschen nicht in Frage, die den harschen AGBs nicht zustimmen (Facebook räumt sich z.B. das Recht ein, Profilfotos auf unbestimmte Zeit für maßgeschneiderte Werbung einzusetzen).

Unternehmen der "Sharing Economy" nach Silicon-Valley-Art schalten sich zwischen private Beziehungen, um diese zu monetarisieren. Damit saugen sie die Gesellschaft aus, bedienen sich ihrer und lassen eine leere digitalisierte Hülle zurück. Der Volkswirtschaft geben sie sehr wenig zurück<sup>2</sup>.

---

<sup>2</sup> <http://www.spiegel.de/wirtschaft/unternehmen/airbnb-zahlt-in-frankreich-nur-70-000-euro-steuern-a-1107259.html>

Es handelt sich also bei diesen Plattformen um asoziale Medien, die als warnendes Beispiel für eine misslungene Digitalisierungsstrategie verstanden werden sollten und nicht als Modell.

### **Wider den unverantwortlichen Einsatz "Sozialer Medien" durch öffentliche Stellen**

Solche Plattformen sind keinesfalls angemessenen Medien für die Kommunikation zwischen Behörden oder Institutionen und Bürgern. Vor dem Hintergrund, dass manche Polizeibehörden inzwischen Twitter für einen geeigneten Kanal für aktuelle Informationen, Fahndungsaufrufe und sogar Weisungen an Demonstrationen<sup>3</sup> halten, mahnen wir für solche Zwecke die Schaffung und ausschließliche Nutzung einer akzeptablen Alternative an. Es ist dem geneigten Bürger durchaus zuzutrauen und zuzumuten, einmal eine andere URL als die von Twitter einzugeben, um die Meldungen der Polizei zu empfangen.

Der Einsatz von "sozialen Medien" für die Öffentlichkeitsarbeit ist im Regelfall völlig inakzeptabel, weil Unternehmen wie Twitter keine neutralen, allen gleichermaßen zugänglichen Plattformen und auch keine neutralen Überträger von Nachrichten sind. Im Gegenteil, sie allein bestimmen, wer sich anmelden darf und wer welche Nachricht wann sieht - und sehen sich dabei unter Umständen nicht einmal klar an deutsches (Datenschutz-)Recht gebunden.

Wir schlagen vor, dies im Entwurf zu thematisieren und ihn so abzuändern, dass er für solche Zwecke explizit die Förderung von auf freier Software basierenden Plattformen vorsieht. Für die Öffentlichkeitsarbeit käme eventuell eine von einem öffentlichen Träger betriebene Instanz eines nicht proprietären Netzwerkes in Frage - neben klassischen Pressekonferenzen und Sprechstunden.

### **Hieraus ergibt sich eine unerlässliche Ergänzung zu Abschnitt 4:**

#### **Kritischer Umgang mit Informationstechnologie in der Schule - in jeder Hinsicht**

Ein unerlässlicher Teil der Medienkompetenz ist die Entwicklung eines kritischen Bewusstseins gegenüber der Struktur, Methoden und Ziele der Medien. Dies trifft in besonderem Maße aufs Digitale zu. "Soziale Medien" haben an Schulen nichts zu suchen, wenn es sich dabei um die oben beschriebenen asozialen Medien handelt. Es sind keine Werkzeuge, sondern interessierte Akteure, die arglistig junge Menschen mit ihrer Ideologie durchdringen möchten, zum Zwecke der profitorientierten Verhaltensmanipulation.

---

<sup>3</sup> <https://netzpolitik.org/2014/entfernen-sie-sich-bitte-in-die-angegebenen-richtungen-berliner-polizei-nutzt-twitter-fuer-durchsagen-an-demonstrierende/>

Unternehmen wie Facebook zielen auf eine junge Zielgruppe - eine Strategie, die der der Tabakindustrie<sup>4</sup> ähnelt. Sie setzen auf sozialen Druck oder verführen durch falsche Versprechen zum Mitmachen - eine Strategie, die den Machenschaften von Kulturen, Sekten und Schneeballsystemen ähnelt. So präsentiert Facebook Menschen, die nicht mehr teilnehmen wollen, emotional erpresserische Behauptungen, ihre Freunde würden "traurig" werden oder "sie nicht mehr kontaktieren können", falls sie mit der Schließung ihres Profils Ernst machten - unter jedem Portrait eine andere (erfundene!) Botschaft.

Die Marketingstrategien der Tabakindustrie und emotionale Manipulation durch Sekten sind mittlerweile mit Recht verpönt - die der noch viel schädlicheren Datenindustrie, die ihr Geld durch amoralische Verhaltensmanipulation (i.e. Werbung) macht und somit beliebigen anderen Machenschaften zum Erfolg verhelfen kann, erfährt momentan leider politischen Aufwind und wird immer noch viel zu unkritisch betrachtet.

Der Tendenz, die angeblichen "Werkzeuge" der "sozialen Medien" in den Schulbetrieb (Organisation und Unterricht) einzubinden, ist aus diesem Grund unbedingt ein Riegel vorzuschieben. Die ständige Vernetzung, das ständige unreflektierte Weitergeben aller Erfahrungen, die dann für immer gespeichert werden, ist ein Risiko für die Persönlichkeitsentwicklung.

Sich keine Gedanken zu machen, bevor eine Emotion, ein Gedanke oder eine Erfahrung "geteilt" werden - so dass diese zu Marketing- und allen anderen Zwecken, die sich in Zukunft ergeben können, in einer ewigen und unendlich detaillierten Akte gespeichert werden - ist eine Ideologie, die die "sozialen Medien" vermitteln. Es handelt sich also um alles andere als "wertfreie Werkzeuge". Es muss klar sein, dass man darüber weder Lerngruppen noch Klassenreisen organisieren darf.

In gar keinem Fall darf der Unterricht, auch nur zu einem noch so kleinen Teil, "über Facebook" ablaufen, auch dann nicht, wenn Schulleitung und Eltern diesen Wunsch äußern sollten: es die Daten der SchülerInnen, die erfasst werden. Diese können aber noch kein informiertes Einverständnis geben: zu den Spätfolgen durch digitale Daten-Altlasten wird noch wenig geforscht. Sicher ist aber, dass ein durchschnittliches Facebook-Dossier weitaus umfangreicher und aufschlussreicher ist als eine Stasi-Akte<sup>5</sup>.

---

4 [https://www.dkfz.de/de/tabakkontrolle/download/Publikationen/RoteReihe/Band\\_18\\_Zigarettenwerbung\\_in\\_Deutschland.pdf](https://www.dkfz.de/de/tabakkontrolle/download/Publikationen/RoteReihe/Band_18_Zigarettenwerbung_in_Deutschland.pdf)

5 <http://europe-v-facebook.org/DE/Datenbestand/datenbestand.html>

Gerade an Schulen ist es dagegen wichtig und dringlich, über die Macht von Datengiganten, vorgeblichen "sozialen" Medien oder Netzwerken und Werbeindustrie aufzuklären und entsprechende Projekte (in Zukunft vielleicht sogar Ausstiegsprojekte) zu fördern. Die Vorteile können stets auch durch institutionslokale bzw. Peer-to-Peer-Lösungen erreicht werden, die im Unterricht auch unbedingt diskutiert werden sollten - übergeordnet ist das Recht auf analoge Teilhabe zu respektieren und zu vermitteln.

Da hilft ein Aufspringen der Schulen auf digitale Hypes - die Benutzung des Digitalen um des Digitalen willen, nur weil es modern ist - wenig; werden nur die führenden Marken in den Köpfen etabliert, steht die oberflächliche Benutzung im Vordergrund, so führt das unweigerlich zu unkritischer Verwendung.

Ein viel sinnvollerer Bildungsziel als der oberflächliche "Umgang" mit gängigen (kommerziellen) Programmen und mit der ständigen Vernetzung ist vielmehr, die darunterliegenden Strukturen zu verstehen. Viel sinnvoller ist es also, im Informatikunterricht die Fähigkeit und die Begeisterung dafür zu vermitteln, unter die Oberfläche zu schauen. Soft- und Hardware auseinanderzunehmen und selbstbestimmte Vernetzungsmodelle zu betrachten und ein Bewusstsein für Datenschutz und -sicherheit zu fördern.

Ein solches Unterrichtsziel geht über bloße Medienkompetenz hinaus. Diese ist ebenfalls äußerst wichtig ist, wie der Entwurf bereits korrekt ausführt; komplementiert werden muss sie in Zukunft aber durch eine kritische Auseinandersetzung mit der Technologie, in der die Medien implementiert sind, sowie den wirtschaftlichen Zusammenhängen dahinter.

Entsprechende gemeinnützige Initiativen existieren (beispielsweise das Projekt "Chaos macht Schule" des CCC e.V.<sup>6</sup>) und wir empfehlen dringend, diese als Modell zu begreifen. Nichts ist entscheidender für die Zukunft als die Schulbildung, die stets zu kritischen und mündigen Bürgern erziehen muss.

Nur durch den Blick unter die Oberfläche wird in Schleswig-Holstein eine Generation heranwachsen, die Gestalter und nicht Spielball der Digitalisierung ist.

---

6 <https://ccc.de/schule>

### **Zu Punkt 3.3:**

Auch in der Arbeitswelt führt eine vermeintlich bessere Planung dazu, dass Arbeitsplätze vernichtet werden und durch die Flexibilisierung der verbleibenden Jobs soziale Errungenschaften verlorengehen (Scheinselbständigkeit, absurde hyperflexible Arbeitszeiten in vielen Betrieben<sup>7</sup>). Durch eine sekundengenau auswertbare Überwachung des Kommunikationsverhaltens, wie sie etwa durch IBM angeboten wird, können Angepasstheits-Metriken definiert werden, nach denen Angestellte von Vorgesetzten (bzw. durch die Algorithmen von IBM) willkürlich beurteilt und bestraft werden. Wenn das die "Zukunft der Arbeit" ist, dann ist die Zukunft der Arbeit wieder eine neue Ausprägung von Sklaverei in Form einer unablässig verlangten Selbstoptimierung.

Dass die "Beschäftigten in den Wandel einbezogen" werden sollen, ist nett gemeint, reicht aber nicht: auch durch Mobbing und Bossing seitens einer Mehrheit, die sich persönliche Vorteile verspricht, kann ein Konsens zur persönlichen "Digitalisierung" hergestellt werden - wir kennen Berichte aus Unternehmen, in denen Mitarbeiter durch Führungskräfte angehalten werden, sich privat in "sozialen Netzwerken" aufzuhalten, was leider von einer Mehrheit widerstandslos mitgetragen wird. Einzelne Mitarbeiter und sogar Betriebsräte und Datenschutzbeauftragte sind dagegen faktisch machtlos.

Automatisierung und Robotik bargen das Versprechen, den Menschen Arbeiten abzunehmen. Lasse sich der Mensch stattdessen zum Sklaven, zur Marionette der Technologie machen, stimmt etwas an den gesellschaftlichen Zielsetzungen nicht. Erklärbar ist der Effekt dadurch, wenn Effizienzsteigerungen durch Wachstum aufgefressen werden und wenn sich der Mensch als Objekt im Modell befindet, obwohl er eigentlich Subjekt sein sollte und die technologische Entwicklung der gesellschaftlichen dienen und folgen sollte, anstatt sie zu formen.

Diese Art Wandel bedarf also keiner "Leitplanken" auf ihrem anscheinend unaufhaltbaren Weg, sondern einer gesellschaftlichen Besinnung und deswegen einer Bremse. Arbeitsplätze dürfen nicht weiter aus Wachstumsgründen digitalisiert und flexibilisiert werden. Die unaufhaltbare Schneise der Digitalisierung ist kein Naturgesetz, sondern die Summe allzu zaghafter Entscheidungen.

Die erwähnte "Automatisierung der Arbeitswelt" ist also eine entscheidende Weiche. Nur wenn Menschen bei der Automatisierung von Prozessen nicht einfach als Ressourcen in ein berechenbares Modell einbezogen werden dürfen, gelingt sie. Nur wenn tatsächlich eine Verringerung der Wochenarbeitszeit, der fremdbestimmten Arbeit dabei herauskommt, hat sich die Automatisierung gelohnt. Ansonsten stellt sich wiederum die Frage: wenn sie nicht uns (den Menschen, der Gesellschaft) dient, wem dient sie?

---

<sup>7</sup> <https://populardemocracy.org/news-and-publications/starbucks-workers-confront-executives-demand-scheduling-reform>



Das Schlagwort "Industrie 4.0" wäre aus dem Entwurf zu streichen, weil es Zusammenhänge vernebelt und vermengt. Geht es im Kern einfach um flexible Fertigungsverfahren und Zulieferungsketten, dann sollte man sie so nennen. Digitale Vernetzung allein ist für die Allgemeinheit kein Selbstwert und schafft mindestens drei gewichtige neue Problemfelder: IT-Sicherheit, Übergriffe der Berufswelt auf das Privatleben, Verbreitung drahtlos kommunizierender Dinge außerhalb der Fabrik (z.B. Kleidung, die noch RFID-Chips enthält).

### **Generell zum Thema Wirtschaft, Gründungen und Industrie:**

Auch unter ethisch begründeten Rahmenbedingungen können Gründungen im digitalen Sektor funktionieren. Durch eine verstärkte Ausrichtung hin zu ethischer Datenverarbeitung wird Schleswig-Holstein eine Führungsrolle übernehmen, selbst wenn die sogenannte "Sharing Economy" sich als eine Blase herausstellen sollte. Der kluge Umgang mit Informationstechnik setzt immer eine ethische Dimension voraus. Diese fehlt dem Silicon-Valley-Modell der "disruptiven" Digitalisierung bzw. gerät zu einem plakativen: "Wir machen Euer Leben besser, so wie wir es für richtig halten. Widerstand ist zwecklos".

Die ethische Dimension sollte uns nicht fehlen und steht auch nicht in Widerspruch zu Punkt 3.2, sondern ist vielmehr eine notwendige Ergänzung zu Punkt 3.2.4.: Mit unseren Daten wird nicht experimentiert.

### **Zum Begriff der "künstlichen Intelligenz", "smarter" Umgebung und selbstfahrenden Autos**

#### **Punkt 1: "Künstliche Intelligenz" und "Ambient Assisted Living"**

Die Begriffe "Künstliche Intelligenz" und "Ambient Assisted Living" suggerieren absurde Heilsversprechungen. Die erste Problematik steckt bereits im Begriff "künstliche Intelligenz", der allzuleicht die Fähigkeit angedichtet wird, echtes menschliches Verstehen ersetzen zu können. Die zweite Problematik ist die bei halbgaren "Visionen" wie dem sogenannten "Ambient Assisted Living" stets mitschwingende Zielsetzung: den Menschen durch die Ersetzung von "teurem" Pflegepersonal durch kalt rechnende Maschinen aus dem Funktionieren einer menschlichen Gesellschaft wegzurationalisieren. Dies ist an Zynismus und Absurdität nicht zu überbieten. Sollte uns nicht gerade durch die Automatisierung mehr Zeit für das Miteinander bleiben, dann ist nicht klar, welchem Zweck sie überhaupt dienen mag.

Wer sogenannte "künstliche Intelligenz" als einen unverzichtbaren Bestandteil der Zukunft sieht, überschätzt deren Fähigkeiten. Die Vorstellung, Menschen über ihr elektronisch aufgezeichnetes Verhalten modellieren zu wollen, ist reine technologische Hybris. Eine Nutzungsoberfläche, die den Nutzer modellieren und "vorausberechnen" will, kann auf ganz neue Arten unbrauchbar sein: anstatt sich eines Knopfes mit einer klar definierten Wirkung bedienen zu können, muss der Nutzer nun auf Schritt und Tritt raten, was bei einer bestimmten Handlung geschehen wird. Es ist nämlich (glücklicherweise) allgemein unmöglich, menschliches Denken in mehr als einem statistischen Sinn durch berechenbare Modelle zu erfassen.

Sogar das flott daherkommende "Ambient Assisted Living" kann leicht in ein alpträumhaftes Szenario umkippen, in dem die häusliche und städtische Umgebung den Bewohnern implizit vorschreibt, auf welche Weise sie sich zu bewegen und zu verhalten haben, um Schwierigkeiten zu vermeiden. Eine menschliche Instanz, an die sie sich unmittelbar wenden können, fehlt - wurde eingespart - und könnte vermutlich auch nicht die richtigen Einstellungen treffen, ohne zu raten. Solche Projekte bleiben hoffentlich Spielereien. "Das Wohnen der Zukunft", auch für Senioren, stellen wir uns anders vor. Das Wegrationalisieren des Menschen aus dem Funktionieren einer menschlichen Gesellschaft ist ein widersinniges, abstruses Ziel.

"Künstliche Intelligenz" ist eben keine Intelligenz, sondern ein Schema zur Datenverarbeitung. Sie versteht nichts und sie kann nicht korrekt auf etwas reagieren, das sich außerhalb ihres Modells abspielt - das gilt selbst für Go-spielende Supercomputer und andere Wunderwerke der Technik. Sie werden unsere Probleme nicht für uns lösen.

Von der Unterordnung des menschlichen Denkens und Handelns in ein solches Schema, ein Modell, geht eine große Gefahr aus, nämlich dass das Rahmenwerk der Informationstechnologie mit seinen Limitationen das Denken strukturiert. Joseph Weizenbaum, Computerpionier und KI-Kritiker der ersten Stunde, drückte es so aus: "Die Gefahr, dass der Computer so wird wie der Mensch ist nicht so groß, wie die Gefahr, dass der Mensch so wird wie der Computer".

## **Punkt 2: Selbstfahrender Verkehr vs. Abkehr von der Auto-Stadt**

Durch die Beschränkungen der KI verbietet sich auch der (im Entwurf kurz erwähnte) Einsatz selbstfahrender Autos. Anders als beim Autopiloten eines Flugzeugs müsste ihr Autopilot über Situationen entscheiden, die Computer auf absehbare Zeit nicht abstrahieren können - weil sie nichts verstehen. Stadtverkehr lasse sich nur dann automatisieren, wenn Fußgänger- und RadfahrerInnen zu reinen Störfaktoren erklärt werden, die nur in dem Maße geschützt werden können (schützenswert sind?), in dem ihr Datenschatten durch den vorgeblich "intelligenten" selbstfahrenden Verkehr erkannt und verarbeitet werden kann.

Erstens muss die Frage erlaubt sein, was mit den massiv anfallenden Daten passiert und ob ihre Erhebung durch die angeblichen (von interessierten Seiten prognostizierten!) Vorteile selbstfahrender Autos zweifelsfrei gerechtfertigt sind. So ist nicht nur die klassische Videoüberwachungsproblematik vorprogrammiert, sondern auch eine Einbeziehung von personenbezogenen Daten etwa in die Routenplanung leicht machbar. So kann gegen ärmere NutzerInnen nahezu unsichtbar diskriminiert werden.

Der zweite Einwand gegen selbstfahrenden Verkehr ist noch schwerwiegender. Öffentliche Wege müssen für nicht-vernetzte oder aus anderen Gründen weniger gut computer-erkennbare Menschen benutzbar bleiben, ohne dass die Gefahr besteht, dass ein Autopilot sie in seinem Modell als weniger schützenswert ansieht als ihre "Smartphone"-tragenden, ideellen bzw. modellgerechten Gesichts-, Bewegungs- und Körpermodellen entsprechenden Mitmenschen.

Im Klartext: jede Entscheidung der Maschine muss aufgrund von Sensordaten fallen, die physikalische Werte (Lichteinfall, Radarecho usw.) abbilden. Diskriminierung aufgrund körperlicher Behinderungen, Körpermaße, Kleidung, Aussehen (oder beispielsweise edem Verzicht auf das Aussenden eines Funksignals) ist schwer zu vermeiden. Die Folgen einer Diskriminierung durch die Technik gehen bis zu fahrlässiger Tötung. Das (nicht unabhängig bestätigte) angeblich akkuratere Fahrverhalten heutiger Versuchsmodelle gegenüber menschlichen Fahrern kann nicht über diese Fragen hinwegtrösten.

Mit keiner uns bekannten Technologie ist es ein realistisches Unterfangen, diesem zentralen Punkt - der unbedingten Vermeidung der Diskriminierung gegen nicht dem Modell entsprechenden Menschen - Genüge tun zu wollen, es sei denn, die Straße ist für Menschen generell nicht mehr zugänglich. Ob das aber eine lebenswerte Umgebung ergibt, wagen wir zu bezweifeln: die Auto-Stadt ist nicht ohne Grund ein Auslaufmodell.

Die gewichtigen Vorbehalte gegen selbstfahrenden Verkehr wären beide im Entwurf festzuschreiben, damit in diesem Bereich mehr Wachsamkeit vor katastrophalen Fehlentwicklungen und allzu optimistischen Einschätzungen der Eigenschaften dieser Technologie in das Bewusstsein Einzug hält.

## **Zu den "Vorteilen" erzwungener, personalisierter Messungen**

### **Punkt 1: Zwangsweise Verdatung von Haushalten entzaubert, am Beispiel des Digitalstromzählers**

Alle Verordnungen, die den Einbau oder die Duldung vernetzter Elektronik in der eigenen Wohnung vorschreiben, müssen sofort auf den Prüfstand. Argumentationen, die gegenteilige Entwicklung "nütze doch" den damit Zwangsbeglückten, greifen zu kurz.

Die privatsphäneverletzende Datenerhebung kommt dem "digitalen Wandel", also Partikularinteressen aus der Wirtschaft, zugute. Oft wird argumentiert, dass sie sogar dem Gemeininteresse dienlich sein könnte: nur vernetzte Digitalstromzähler können angeblich das Stromsparen befördern.

Schon diese Aussage ist falsch, denn dazu werden die Messdaten nur lokal gebraucht und es hindert niemand den Verbraucher daran, selbst ein - eventuell subventioniertes - Messgerät einzusetzen. Außerdem müsste der Versorger wirksam daran gehindert werden, verhaltensbasierte Lockangebote zu machen oder den Tarif willkürlich festzulegen. Das ist nicht unwahrscheinlich und wäre schwer nachweisbar: in der Automobilbranche ist Fehlprogrammierung von Steuerungsanlagen in betrügerischer Absicht bekanntlich aktenkundig, durch Programmiertricks wurde ein Aufdecken des Betrugs erschwert.

Im Beispiel des vernetzten Digitalstromzählers dürften also alle erhofften Vorteile dauerhaft durch gewichtige Mängel mehr als aufgewogen werden. Diese Mängel betreffen nicht allein die Privatsphäre. Die systemimmanente höhere Anfälligkeit gegenüber technischen Störungen (z.B. Angriffe aus dem Internet, Ausfälle der Datenverbindung, Programmierfehler) ist unbestreitbar. Die Mängel sind bereits im Konzept angelegt, denn zusätzliche Komplexität sorgt für eine anfälligere Infrastruktur. Das kann in niemandes Interesse sein.

Die Vorteile selbst sind zweifelhaft bis überschaubar. Sie sind auch abhängig vom modellgemäßen Handeln aller Beteiligten. Einfache, analoge Technologie ist in Wahrheit gut genug, um den Verbrauch zu zählen. Die Idee, irgendeinen Effekt durch möglichst genaue fremdbestimmte Erfassung erzielen zu wollen, ist obendrein zutiefst undemokratisch: sie legt eine erhebliche Macht in die Hände derer, die diese Daten sammeln. Das sind aber wiederum die Betreiber sowie alle anderen Abnehmer gestohlener Daten, die der Datenkapitalismus kennt.

Selbst wenn die versprochenen Vorteile nun in einzelnen Fällen messbar sein sollten, muss trotzdem dem Wunsch nach der einfachen Steuerbarkeit der Gesellschaft über digitale Regelkreise unbedingt ein Riegel vorgeschoben werden. Vernetzung von Haushalten und Menschen muss auf freiwilliger Partizipation beruhen, das ist der Inhalt des von uns geforderten und begründeten Rechtes auf analoge Teilhabe.

Abgesehen von der bislang fehlenden Interessenabwägung ist es bei der Bewertung von Vorhaben wie dem Digitalstromzähler-Rollout auch nicht ganz unerheblich, dass weder Prognosen, White papers und rosige Versprechungen keinesfalls mit Fakten gleichzusetzen sind.

Abschließend zum Thema Digitalstromzähler: andere Mittel sind tauglicher und hätten eine bessere Steuerungswirkung auf alle Beteiligten: wie wäre es beispielsweise, wenn fossile Energien mit ihren tatsächlichen Kosten berechnet würden?

Die Ersparnis müsste zwangsläufig substantiell sein, denn fossiler Strom würde von einem Tag auf den Anderen unbezahlbar. Die versprochene minimale Ersparnis durch schnüffelnde Stromzähler (wenn sie tatsächlich messbar sein sollte) lohnt sich im Vergleich kaum.

Ohne ein fundamentales Umdenken geht es nicht weiter. Das Wachstum wird optimiert und sogar mit "Umweltschutz" begründet, aber damit belügen wir uns selbst.

Doch mutige, beherzte, wirksame Schritte sind schwerer zu vermitteln und haben auch keine Rückendeckung aus der Industrie. Mikrooptimierung durch schnüffelnde Elektronik bringt nichts, zerstört die Privatsphäre, ist aber eine Einnahmequelle für die Hersteller dieser Elektronik. Aus diesen Gründen ist sie abzulehnen.

## **Punkt 2: Digitalisierung im Gesundheitswesen entzaubert**

Auch "E-Health" ist in der Tat eine Chance. Aber nicht für PatientInnen, die persönliche ärztliche Betreuung und kein bloßes "Management" brauchen und auch keine vernetzten Medizingeräte, "Wearables" oder Implantate. Sie ist primär eine Chance für Datenhaie und gewinnorientierte Versicherungsunternehmen, die ihren Kundenstamm endgültig zu desolidarisierten Selbstoptimierungsrobotern umerziehen wollen<sup>8</sup>. Nichts daran ist wünschenswert.

Informationstechnologie ist ein Mittel, um Skaleneffekte auszunutzen. Die Effizienzsteigerung geht mit kleinstteiliger Verwertbarmachung einher, das liegt in der Natur der Datenverarbeitung ("Big Data"). Dieser Tendenz muss entschieden entgegengearbeitet werden. Der Entwicklungen hin zu Effizienz und Profit um jeden Preis muss Einhalt geboten werden, auch und gerade im Gesundheitsbereich.

Eine hastige Digitalisierung, bei der alles erlaubt ist (außer sich ihrer zu erwehren), ist keine gelungene Digitalisierung. Eine gelungene Digitalisierung ist eine, die den Menschen oder den Haushalt niemals als ein Element in einem Regelkreis betrachtet und auch nicht als Versuchskaninchen.

### **Zu den Punkten 2.1.6 und 2.4:**

Bei der Digitalisierung in Behörden sollte Vorsicht das oberste Gebot sein, es sollten nicht überhastet und ohne ernsthafte unabhängige Expertenbegleitung elektronische Akten und Übermittlungsverfahren eingeführt werden. Bei der Einführung der "DE-Mail" wurden Gutachten des CCC e.V.<sup>9</sup> und anderer kritischer Organisationen zwar eingeholt, aber von der Bundesregierung vorsätzlich ignoriert. Das darf sich nicht wiederholen. Wo es um einen Standard für rechtsverbindliche Behördenkommunikation oder um elektronische Strafprozessakten - äußerst sensible Bereiche - geht, muss der Gesetzgeber der Kritik aufmerksam zuhören - und es richtig machen, ohne vorgefasste Entschlüsse.

Mit der elektronischen Aktenführung sollte erst begonnen werden, wenn die technischen Voraussetzungen für tatsächlich prägnant große Datensicherheit stehen. Mehr gibt es dazu momentan angesichts weit verbreiteter Sicherheitslücken, mehr "wollen als können" nicht zu sagen. Wichtig ist dabei, dass anders als bei der "DE-Mail" vorgegangen wird und der Gesetzgeber sich nicht der Illusion hingibt, es gäbe so etwas wie Datensicherheit per Dekret.

---

<sup>8</sup> <http://www.bpb.de/gesellschaft/medien/medienpolitik/236524/internet-der-dinge?p=all>

<sup>9</sup> <https://www.ccc.de/de/updates/2013/de-mail-unqualifizierte-makulatur>

Dazu brauchen wir kein "Cyber-Abwehrzentrum", vielmehr sollten in Ausschreibungen Pentests und andere Qualitätssicherungsmaßnahmen vorgesehen werden. Statt eines "Cyber-Abwehrzentrums" sollte ein offen und transparent arbeitendes, keinem Ministerium unterstehendes CERT eingerichtet werden und Sicherheitsschulungen bei allen Behörden und Betreibern kritischer Infrastruktur vorgesehen werden.

Dieses Landes-CERT müsste deshalb transparent und strikt unabhängig arbeiten, weil die politische Instrumentalisierung von "Cyberabwehr" enorme Gefahren bis hin zum Auslösen eines Krieges aufgrund extrem leicht manipulierbarer<sup>10</sup> "Beweise" dient. Cyberkriegsrhetorik ist un-, ja kontraproduktiv (weil Gelder falsch verteilt werden) und obendrein ein gefährliches Spiel mit der öffentlichen Sicherheit.

Es muss ein klares Verständnis dafür gewonnen werden, dass die Sicherheit von IT-Systemen in der Verantwortung derer liegt, die sie betreiben - derer, die ihren Einsatz verordnen - und derer, die sie entwerfen, implementieren und fortlaufend weiterentwickeln.

Jedwede vorgebliche "Cybersicherheitsstrategie", die reißerisch "Cyber-Angriffe" als das primäre Problem hinstellt, ist zu 100% Show. Eine gute Strategie ist politisch unabhängig und konzentriert sich auf eine Reduktion der Angriffsfläche, ordentliche Kryptographie und das Abdichten von Sicherheitslücken und macht damit die Infrastruktur für alle sicherer, die sie nutzen.

Nicht nur in diesem Zusammenhang begrüßen wir die Ausführungen in Punkt 2.1.7 des Entwurfs und raten zu folgender Verschärfung: allen öffentlichen Institutionen sollte der Einsatz nicht-quelloffener und nicht-freier Software untersagt werden. Geschäftsgeheimnisse machen Systeme nicht sicherer, sie machen lediglich ihre Lücken weniger offensichtlich und behindern im Extremfall ihre Behebung.

Anders als im Schach gilt in der IT-Sicherheit nämlich: Angriff ist keinesfalls die beste Verteidigung. Militärische Metaphern zum "Cyber" wirken auf Fachkundige eher lächerlich (wie soll ein "Gegenangriff" aussehen und was soll er bringen, nachdem der Schaden schon geschehen ist?) und lenken von der Idee ab, dass der Einsatz von IT-Systemen wohlüberlegt sein will, Verantwortungsfragen im Vorfeld geklärt und eher ausreichend Mittel in defensive Sicherheit, die mehr mit Qualitätssicherung als mit Schützengräben zu tun hat, investiert werden sollten.

---

10 <http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382#.VJIH4sgA>

### **Zu Punkt 6.3.3, Single-Sign-On zur Legitimierung sowie digitalen Medien in der universitären Lehre:**

Ein SSO-System für Studierende darf nicht zu einer lückenlosen Überwachung führen. In dem Entwurf wird außerdem fälschlicherweise vorausgesetzt, alle für Studierende relevanten Leistungen der Universität bedürfen einer "Identifizierung". Das ist ein häufiger Fehler, den es zu vermeiden gilt. Der Begriff sollte durch "Authentifizierung" ersetzt werden, die nämlich nicht zwingend eine Identitätsfeststellung impliziert. Berechtigungen können so datenschutzfreundlich geprüft werden<sup>11</sup>.

Es bleibt die Frage, wie oft und wozu Berechtigungen überhaupt abgeprüft werden sollten. Digitale Technik lässt dies in unbegrenzter Kleinteiligkeit zu. Mehr dazu unter "Digitalisierung und kleinteiliges Berechtigungsmanagement"

Um nur ein überraschend häufiges, wenn auch für sich genommen relativ harmloses, Ärgernis dieser Art zu nennen: eine Universität hat vernünftigerweise auch Gästen gegenüber, die beispielsweise nicht die richtige Mensa-Chipkarte besitzen, offen und einladend zu sein. An manchen Instituten ist das aber ein Problem.

Zu digitalen Medien ist anzumerken, dass Forschung und Lehre auch und gerade außerhalb von einengenden digitalen Kontexten erfolgreich ablaufen. Digitalen und virtuellen Angeboten kann höchstens eine komplementierende Funktion zukommen, sie ersetzen nie die analoge und reale Auseinandersetzung mit dem Stoff. Auch die unbedingte Verknüpfung von Kursen mit einem starren Studien-Management-System führt in der Praxis zu unnötigen Erschwernissen sowohl für Lehrende als auch für Studierende - Forschung und Lehre leben von Offenheit und Freiräumen, die durch in Mikromanagement umschlagende Strukturierung leicht erstickt werden.

### **Zu Punkt 8.4:**

Wir halten das flächendeckende Etablieren von Datenerfassung für widersinnig und menschenrechtswidrig. Überlegungen, Landwirtschaft noch weiter zu industrialisieren halten wir für überholt und für Größenwahnsinn.

---

<sup>11</sup> <https://www.irmacard.org/>



Die Auswüchse der industriellen Landwirtschaft managen nur scheinbar unsere Lebensgrundlage, in Wahrheit zerstören sie sie durch Monokulturen und eine alles andere als nachhaltige Ertragssteigerung durch Überdüngung, Auslaugung des Bodens, Gentechnik und Pestizide sowie eine völlig unsinnige Ausrichtung auf Fleischerzeugung: alles Punkte, die sich wunderbar durch die Regelkreise der Optimierung "rechtfertigen" und gewiss durch Daten noch viel effizienter beschleunigen ließen! Und genau dadurch eindrucksvoll zeigen, dass "gemessen" nicht automatisch "smart" ist - und dass all die Technik uns kein kritisches Nachdenken über die Zielvorgaben ersetzen kann.

Zuerst einmal wäre also das Schlagwort "smart" ist aus dem Entwurf zu streichen, weil es Zusammenhänge vernebelt und den Verzicht auf das absurde, störanfällige Einsammeln kleinstteiliger Messwerte - also die robuste Alternative zur hochgezüchteten High-Tech-Welt - für dumm erklärt. Ist das gerechtfertigt? Kaum:

- Um zu erkennen, dass es Tieren in einem Stall nicht gut geht, braucht man keine elektronische Bewegungserfassung. Eine solche Entrückung von der Realität grenzt an Wahnsinn.
- Der Mehrwert der Messwerte ist vernachlässigbar, wenn die Modellannahmen nicht stimmen. Optimieren lassen sich auch unsinnige Kennzahlen: auch Rentabilität auf Kosten der Ökologie ist immer das Ergebnis einer Optimierung.
- Eine Gesellschaft sollte sich - auch in der Nahrungsmittelproduktion - nicht ausschließlich auf eine hochgezüchtete Technologie verlassen, sondern auf eine Vielfalt von Möglichkeiten. Wer neue Technologien ausprobieren möchte, soll dies im Rahmen des Umwelt-, Arbeitnehmer- und Tierschutzes tun dürfen. Das Wort "flächendeckend" ist jedoch unbedingt aus dem Entwurf zu streichen.

### **Zu Punkt 12.1:**

"Vernetzte Mobilität" durch Telematik darf nicht dazu führen, dass Bewegungsprofile angelegt werden oder die Möglichkeit dazu geschaffen wird. Bei all der Begeisterung für Echtzeitdaten darf Anonymität nicht auf der Strecke bleiben. Jede Datenerhebung ist auch in Hinblick auf Auswertungs- und Deanonymisierungsmöglichkeiten zu untersuchen, die sich erst in der aggregierten Datenmenge ergeben.

Alle Verordnungen, die den Einbau oder die Duldung Information drahtlos nach außen tragender oder auf Vorrat speichernder Elektronik im eigenen Fahrzeug vorschreiben, müssen sofort auf einen kritischen Prüfstand mit wachsamem und weitem Blick auf die Folgen dieser Entwicklungen. Sämtliche Telematik muss datenschutzfreundlich angelegt werden, sämtliche allgemeine Überwachung in und von Verkehrsmitteln gehört konkret verboten. Diese Punkte kommen im Entwurf zu kurz.

### **Warum ist der Zweck der Verdattung für uns nicht bewertungsentscheidend?**

In dem Maße, in dem Alltag, Infrastruktur und sogar der besonders schützenswerte Kernbereich der intimen Lebensführung aus irgendwelchen Gründen mit Mess- und Rückwirkungsmöglichkeiten durchzogen werden, nimmt der Spielraum für selbstbestimmtes Leben ab, und zwar über eine Vielzahl von Wegen:

Für jedes einmal gesammelte und auf Vorrat gespeicherte Messdatum lassen sich im Nachhinein weitere Verwendungen finden lassen. Ob diese Verwendungen legal sind, illegal oder in einer Grauzone, würde nur in einer idealen Phantasiewelt eine Rolle spielen. In Realität ist es für Betroffene nicht einfach, die Verarbeitung und Weitergabe von Daten mit Personenbezug vor Gericht im Einzelnen nachzuverfolgen und nachzuweisen.

Jede Rückwirkungsmöglichkeit bedeutet selbst dann eine konkrete Einschränkung der Freiheit und damit der Lebensqualität, wenn sie vorgeblich noch nicht genutzt wird. Selbst die reine Datensammlung hat diese Qualität - da nicht bekannt und nicht wissbar ist, ob später eine Rückwirkungsmöglichkeit geschaffen wird: "chilling effects".

Dies ist bei der Schaffung neuer Messmöglichkeiten immer zu beachten. Am Beispiel der sogenannten "Section Control" kann der Effekt verdeutlicht werden. Erst automatisierte, vernetzte Datenerhebung und -auswertung macht es möglich, Kennzeichenscans für die Geschwindigkeitsmessung zu gebrauchen. Nun ist es, wenn die Messung durch Kameras erfolgt und gleich noch ein persönliches Merkmal aufgezeichnet wird, ein Leichtes, die anfallenden Daten einfach nicht zu löschen sondern zu missbrauchen - und zwar wiederum automatisch.

Bei der Entscheidung für diese Technologie spielte Respekt für die Rechte der betroffenen (regelkonform fahrenden Individuen) also höchstens eine untergeordnete Rolle. Ansonsten hätte man eine datenärmere Variante gewählt, die zwar eventuell nicht alle Vorzüge der neuen Technik hat, aber dafür nicht so leicht zu einer Überwachungsmaschine gemacht werden kann.

Befinden sich solche vermeintlich "gutartigen" Technologien nun überall im Hintergrund, so existiert überhaupt kein Entfaltungsraum für die Persönlichkeit mehr, weil jeder Mensch zu jeder Zeit damit rechnen muss, dass all seine Lebensäußerungen aufgezeichnet und - dies ist die Logik des "Datenreichtums" - später, auch von Dritten, ausgewertet werden.

### **Problemverschärfungen durch kleinteiliges Berechtigungsmanagement**

Es sei ausdrücklich davor gewarnt, für Leistungen stets misstrauisch die Legitimation abzuprüfen, wie es digitale Technik in besonderer Weise erlaubt und befördert.

Die Gefahr ist groß, dass Digitalisierung dazu verleitet, vermeintliche Leistungerschleichung in ungekannter Engmaschigkeit verhindern zu wollen. Dieser Ansatz ist aus verschiedenen Gründen verfehlt. Insbesondere da dieser Entwicklung von technologischer Seite kaum Grenzen gesetzt sind, sind neue Denkansätze gefragt. Es muss bei jeder Leistung, die unter digitale Kontrolle gestellt werden soll, hinterfragt werden, wie groß der gesellschaftliche Nutzen und das volkswirtschaftliche Interesse an der genauen Verfolgung ist. Im Zweifel ist der Freiheit der Vorzug zu geben, auch wenn einzelne "Missbrauchs"- oder Zweifelsfälle zu erwarten sind.

Für eine gelungene digitale Wende muss geklärt werden, wo die Grenzen der Erfassung und der Verarbeitung von Daten zu Legitimierungszwecken liegen und inwiefern Beschränkungen und Kontrolle - auch wenn diese gerechtfertigt scheinen - in die Systeme direkt eingebaut werden dürfen. Als Beispiel können wir DRM ("Digitales Rechtemanagement", eigentlich korrekter: "digitales Restriktionsmanagement") anführen. Für eine minutiöse Überwachung einer gewissen Interpretation von Urheberrechten müssen sämtliche Vorgänge im Endgerät unter fremdbestimmte Kontrolle gebracht werden - ohne komplette Überwachung und komplette Kontrolle wäre DRM wirkungslos, weil das Kopieren, Bewahren, Weiterverarbeiten, Weitergeben digitaler Dateien die leichteste und grundlegendste Aufgabe eines Computers ist.

Maschinen dürften idealerweise weder über Menschen entscheiden noch zum Zementieren von Ungerechtigkeiten eingesetzt werden. Es dürften keine neuen Privilegien entstehen, bestehende dürften nicht abgebildet werden. Ohne einen Konsens dieser Art riskiert die Gesellschaft, in eine Welt aus digital patrouillierten "Gated Communities" abzudriften.

Einige Entwicklungen durch allzu genaue Kontrolle haben wir schon angeschnitten: die Schere zwischen einer schwindenden Gruppe von Digitalisierungsgewinnlern und durch Computerprogramme ausgebeuteten Arbeitskräften, die sich nicht über Wasser halten können und die sehr wahrscheinliche Diskriminierung im personalisierten Straßenverkehr. Hier entschieden einzugreifen und spezifische, wirksame gesetzliche Regelungen vorzubereiten, wäre kein Modernisierungshemmnis, sondern die Voraussetzung für eine gelungene Entwicklung.

### **Alternativen zum ungebremsten Erheben, Verkaufen und Auswerten von Daten**

Unter Datenkapitalismus verstehen wir ein Gesellschaftssystem, in dem auch persönliche und personenbezogene Daten grundsätzlich erhoben, weiterverarbeitet und -verkauft werden dürfen. Menschen werden damit zwangsläufig vom Individuum zum bloßen Lieferanten von Datenströmen abgewertet. Diese Entwicklung zu verhindern und nicht bloß abzuschwächen, muss Grundlage der Digitalisierungsstrategie bleiben. Politik und Staat dürfen auf keinen Fall zum "Herdenmanager" der Datenindustrie verkommen, sondern müssen allen Sammelbegehren entgegensteuern, auch wenn das Profitinteressen schadet. Profite aus der Kommodifizierung schützenswerter Daten sind schmutzige Profite, mag diese Tatsache durch noch so edle Versprechen (z.B. angeblich bessere Gesundheitsversorgung durch den Verkauf von Patientendaten) kaschiert sein. Sie sind auch ungerecht, weil davon auszugehen ist, dass nur wenige sich vom andauernden "Daten-Aderlass" freikaufen können werden.

Direkte Alternativen zum Datenkapitalismus finden sich etwa in der Entwicklung datenschutz- und privatsphärefreundlicher Methoden, durch die sich etliche der Vorteile retten lassen, der Schutz der Privatsphäre und Sicherheitsaspekte aber den ihnen gebührenden Stellenwert bekommen. In diesem Bereich sind erfolgreiche Gründungen wünschenswert. Warum nicht eine ethische Alternative zu "Big Data" fördern?

In diesem Zusammenhang ist die Arbeit etwa von Lindell und Pinkas<sup>12</sup> auf dem Gebiet der Secure Multiparty Computation, vielleicht auch das neuere Gebiet der Differential Privacy<sup>13</sup> wegweisend, inzwischen gibt es eine Menge neuer Auswertungsmethoden, die keinen Vollzugriff mehr auf Datenbanken erfordern. All das ist aber Makulatur, wenn nicht auch der Aspekt der Datenerhebung und die Gefahr durch offenliegende Datensilos berücksichtigt werden.

---

12 <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1004&context=jpc>

13 [https://de.wikipedia.org/wiki/Differential\\_Privacy](https://de.wikipedia.org/wiki/Differential_Privacy)

Warum nicht die Verwendung nichtkommerzieller, datenschutzfreundlicherer Alternativen zu den angeblichen "sozialen Medien" fördern, bei denen Nachrichten nicht zentral archiviert und ausgewertet werden?

Was Vernetzung angeht, ist das "Internet of Things" (nicht explizit im Entwurf erwähnt, aber gemeinhin als Teil der "Industrie 4.0" verstanden) nur eine Zukunftsvision von vielen - und zwar aus bereits diskutierten Gründen keine besonders kluge: ein Sicherheits- und Privatsphären-Alptraum, unterm Strich kein echter Mehrwert und Ein Gegenmodell zu einer klugen Digitalisierungsstrategie.

Es ist klug, die Abhängigkeit kritischer Infrastruktur oder des Funktionierens der Gesellschaft von der Informationstechnologie zu reduzieren, anstatt sie zu befördern. Analoge Vorgänge mögen altmodisch und redundant erscheinen - gerade diese Redundanz kann im Falle eines Ausfalls der digitalen Technologie die Folgen abmildern.

Was die Erhebung angeht, genügt oft eine simple Abwägung. So verbieten sich Kameras, wo auch eine Kontaktschleife das gewünschte Ergebnis liefern kann. Es verbieten sich Drohnen, wenn auch ein simpler Kontrollgang es tut. Hier fällt es im Entwurf sehr positiv auf, dass das ULD an vielen Stellen in Entscheidungen und Planungen einbezogen werden soll. Die Einbindung des ULD sollte auf alle Bereiche der Digitalisierung ausgeweitet werden. Auch dort, wo der Datenschutzaspekt zunächst nicht offensichtlich ist, kann er im Verborgenen existieren. Dies liegt in der Natur der Sache, weil digitale Systeme schon heute Einfachheit vortäuschen, aber in Wahrheit hochkomplex sind.

Aus der Kombination von Komplexität und einem dem unbedingten Effizienzgedanken geschuldeten Mangel an (analoger, ohne High-Tech auskommender) Redundanz ergibt sich eine immanente Störanfälligkeit. Aber warum auf komplizierte, störanfällige und hochgezüchtete Systeme setzen, wenn einfache es tun oder wenn das Problem, das sie lösen wollen, vielleicht bei näherem Überlegen gar keines ist? Öfter mal auf einen Trend nicht aufzusteigen, kann langfristig die klügere Wahl sein. Dies betrifft insbesondere die Idee, kritische Infrastruktur vernetzen zu wollen, bevor die Grundlagen der Absicherung geklärt sind.

Man braucht nur die Verlautbarungen aus der Industrie und die oft dicht darauffolgenden Meldungen über kritische Sicherheitslücken gegenüberzustellen, um zu sehen, dass die durch digitale Technologie verursachten Probleme nicht allein durch Marketing, wohlklingende Worte und Gesetze zu regeln sind. Vielmehr bedürfen sie stets einer ausgesprochen überlegten und vorsichtigen Herangehensweise.

In diesem Zusammenhang sei abschließend angemerkt, dass trotz aller "softwaredefinierten" Eigenschaften jede Digitalisierung letztendlich zu 100% abhängig ist von der physischen High-Tech-Industrie und den Mitteln zur Chipproduktion. Ein ernstzunehmender Technologiestandort muss sich Gedanken über die Produktionsmittel machen und eventuell in Zukunft Halbleiterfabriken betreiben, um Einfluss auf technologische Entwicklungen nehmen und im globalen Wettbewerb vorn mitspielen zu können. Möglicherweise ist die Förderung von Unternehmen, die vor Ort vertrauenswürdige Chips herstellen, eine gute Alternative zu Daten-Startups und eine gute Ergänzung zu einer Digitalisierungsstrategie?

### **Im Fazit:**

- Datenerhebung ist immer ein Problem für die Betroffenen, eine Chance ist sie hauptsächlich für diejenigen, die diese Daten auswerten können. Soll die Datenerhebung einem öffentlichen Gut dienen, so müsste dennoch genauestens auf die Möglichkeit persönliche Rückschlüsse geachtet werden. Ansonsten ist sie abzulehnen und von einer Förderung abzusehen.  
Bei einer Interessensabwägung ist die Kehrseite der Daten - um keine zu optimistische Folgenabschätzung zu riskieren - stärker zu gewichten als die Vorteile, die man sich verspricht. Es ist klug, die Abhängigkeit kritischer Infrastruktur oder des Funktionierens der Gesellschaft von der Informationstechnologie zu reduzieren, anstatt sie zu befördern.
- An Schulen muss der kritische Umgang mit Informationstechnologie vermittelt werden, weniger der Umgang mit der Oberfläche.  
Dies ist der wichtigste Kritikpunkt an Abschnitt 4.
- Die Hoheit über das eigene Gerät ist die Grundlage für das Vertrauen in dieses.  
Aufgrund der intimen "Beziehung" von Menschen zu ihren informationsverarbeitenden Geräten ist dieses Postulat absolut und nicht relativierbar und gilt auch für mobile Endgeräte.  
Eine Positionierung gegen DRM und gegen Paragraphen, die das Erforschen von Hard- und Software oder den harmlosen kreativen Umgang damit einschränken, ist daher in einer Digitalisierungsstrategie unerlässlich.

- Datensicherheit ist oberstes Gebot bei der Verwendung von IT in Behörden und Betrieben, der Weg dahin ist aber nicht in Cyber-Abwehrzentren zu suchen, sondern in verantwortlichem Einsatz der Informationstechnologie und im Grundsatz der Datensparsamkeit.  
Daten, die nicht anfallen, werden nicht gestohlen. Geräte, die übers Netzwerk steuerbar sind, sind durch beliebige Akteure mit minimalem Risiko angreifbar.  
Wurden durch einen Angriff sensible Systeme von Behörden oder Industrie kompromittiert, dann ist eine mögliche - aber notorisch schwer ehrlich zu beantwortende - Frage: wer griff an und warum? Die Frage mit dem größeren Nutzwert ist jedoch: waren die betroffenen Systeme nach objektiven Kriterien gut geschützt? Wenn nein, warum hingen diese Systeme derart ungeschützt an einem Netzwerk? Etwa aufgrund überhasteter "Digitalisierung"?
- Die ethische Dimension der Datenverarbeitung sollte uns wichtiger sein als das unbedingte Wachstum schädlicher Wirtschaftszweige, deren Vorteile nicht einmal allen Betroffenen zugute kommen, sondern nach Gutdünken verteilt werden.  
Ein Projekt darf nicht nur an seinen Vorzügen gemessen werden. Der Hinweis, das, was man optimieren wolle, liege im öffentlichen Interesse, genügt nicht, um eine Verdattung zu rechtfertigen.  
Deshalb darf es keine flächendeckende Verordnung zur Datensammlung geben, selbst wenn man sich davon einen besseren Umweltschutz, Brandschutz, besseren Verkehr, straffere Verwaltung oder effizientere Strafverfolgung oder sonstige an sich positiven Effekte verspricht.
- Es gibt vielfältige Alternativen zum ungebremsen "Big Data", das nicht als der einzige Wirtschaftszweig der Zukunft missverstanden werden darf.  
Es gibt auch vielfältige Möglichkeiten, die Vorteile von "sozialen Netzwerken" auf nicht profitgetriebene Weise zu realisieren. Mitnichten ist eine kommerzielle Plattform logisch notwendig, um Nachrichten auszutauschen.
- Nur durch die unbedingte und konkrete Achtung der Menschenwürde gerät die digitale Wende nicht zu einer Dystopie, vor deren Vollendung selbst die ärgsten Befürworter des "Datenreichtums" erschrecken dürften.