

Ein sozialdemokratisches Projekt für den Umgang mit der digitalen Revolution

Jean Christophe Schwaab, August 2018

Inhaltsverzeichnis

Einleitende Bemerkungen	S. 3
1. Auftrag	S. 3
2. Definitionen und Ausgangslage	S. 4
3. Vorteile der digitalen Revolution aus sozialdemokratischer Sicht	S. 5
4. Risiken der digitalen Revolution aus sozialdemokratischer Sicht	S. 7
5. Vorschläge: die Grundrechte an die digitale Revolution anpassen	S. 22
6. Abkürzungen, Bibliographie, Anmerkungen und Verweise	S. 38

Einleitende Bemerkungen

Der Inhalt des vorliegenden Berichts ist politisch und subjektiv, sowohl in der Auswahl der Themen als auch in der Art und Weise, sie zu behandeln. Obwohl ich versucht habe, mich von meinen Standpunkten zu lösen, vor allem dort wo sie von jenen der Partei abweichen (z. B. beim E-Voting), ist nicht auszuschliessen, dass sie in meinen Zeilen durchscheinen. Der Bericht hat auch nicht den Anspruch, erschöpfend zu sein oder jede behandelte Problematik unter allen Gesichtspunkten zu beleuchten bzw. direkt umsetzbare oder zumindest in parlamentarische Vorstösse umwandelbare Lösungen zu präsentieren. Er soll vielmehr als Ausgangspunkt oder eine Art Basislager dienen, um konkretere politische Projekte zu erarbeiten und sich dabei vor allem auf die zitierten, detaillierteren Quellen zu stützen. Zudem werden gewisse, in der Öffentlichkeit wohlbekannte Probleme oder solche, die in anderen Publikationen bereits ausführlich beleuchtet wurden (z. B. die Datenschutzrisiken im Zusammenhang mit der digitalen Revolution oder die Netzneutralität), hier nicht im Detail erläutert. Es war auch schwierig, das Dokument klar zu strukturieren, sind doch die behandelten Themen und Probleme übergreifend und miteinander verknüpft. Ich hoffe, dass die gewählte Struktur lesbar und verständlich ist.

Die genannten Unternehmen, Apps, Softwares, Produkte, Maschinen und andere Roboter sind hier nur beispielhaft aufgeführt, ohne Bewertung ihres Handelns, ihrer Nützlichkeit und ihren Vor- bzw. Nachteilen.

Zwecks besserer Lesbarkeit wurde weitgehend die männliche Form gewählt; sie soll in keiner Weise diskriminierend sein.

Schliesslich geht mein Dank an Min Li Marti, die mir freundlicherweise ihre ausführlichen Anmerkungen zu den Folgen der digitalen Revolution überlassen hat.

1. Auftrag

Wie im Mailverkehr mit Roger Nordmann vereinbart, hier die Ziele des vorliegenden Berichts:

- Aufzeigen der Vorteile und Chancen der digitalen Revolution für die Bevölkerung, das gesellschaftliche Leben, die Behörden und den Wirtschaftsstandort, ohne jedoch in die Verherrlichung im Stil der «Techno-Optimisten» zu verfallen.
- Aufzeigen der Risiken der digitalen Revolution für die gleichen Akteure, ohne jedoch in den Pessimismus à la «1984» oder «Künstliche Intelligenz und Roboter werden die Macht übernehmen und uns die Arbeit wegnehmen» zu verfallen.

2. Definitionen und Ausgangslage

Digitale Revolution

Wikipedia definiert die digitale Revolution wie folgt: «Der Begriff Digitale Revolution bezeichnet den durch Digitaltechnik und Computer ausgelösten Umbruch, der seit Ausgang des 20. Jahrhunderts einen Wandel nahezu aller Lebensbereiche bewirkt und der in eine Digitale Welt führt, ähnlich wie die industrielle Revolution 200 Jahre zuvor in die Industriegesellschaft führte. Deshalb ist auch von einer dritten industriellen Revolution die Rede oder in technischer Hinsicht von mikroelektronischer Revolution. Die mit der Digitalen Revolution einhergehenden Veränderungen in Wirtschafts- und Arbeitswelt, in Öffentlichkeit und Privatleben vollziehen sich in großer Geschwindigkeit überall dort, wo die materiellen Voraussetzungen für Anwendungs- und Nutzungsmöglichkeiten der fortschreitenden Digitalisierung bestehen. Neue Medien beeinflussen zunehmend Kommunikationsverhalten, Sozialisationsprozesse und Sprachkultur».

In diesem Dokument benutzen wir den Begriff «digitale Revolution» als Synonym für «Digitalisierung» (im Sinn eines gesellschaftlichen Wandels und nicht als Umwandlung von Dokumenten in digitale Codes), «digitalen Wandel und Wandel der Gesellschaft und/oder der Wirtschaft», «Aufschwung der neuen Technologien», «[Thema einsetzen] 4.0» usw.

Noch eine digitale Revolution?

Die digitale Revolution ist ein uralter Trend. Seit der Erfindung des Zählrahmens vor über dreitausend Jahren bauten die Menschen Maschinen, die schneller und genauer rechnen konnten als sie selber. Im Lauf der Jahrhunderte tauchten immer neue Rechenmaschinen und -methoden auf, auch solche für die Informationswiedergabe und -verbreitung, zum Teil sehr komplexe und effiziente, die manchmal grosse Veränderungen der Gesellschaft mit sich brachten¹. Zum Beispiel wurde 1805 von Jacquard der mechanische Webstuhl erfunden, er funktionierte bereits mit Hilfe von... Algorithmen²! Der Einsatz neuer Technologien brachte stets Ängste und Kritik oder Verbotsversuche mit sich; schon Platon wollte in seinem «Phaidros» das Aufkommen der Schrift verhindern, weil sie für ihn «unmenschlich» war und «das Gedächtnis zerstörte».

Die digitale Revolution, die wir gegenwärtig erleben, enthält jedoch neue Elemente, die über die Leichtigkeit und Geschwindigkeit, immer komplexere Rechnungen zu bewältigen, weit hinausgehen: Informationen werden vernetzt, gesichert, kombiniert, wiederverwertet. Sie werden auch fälschlicherweise gesichert und aufbewahrt, selbst wenn ihr ursprünglicher Nutzen (im Sinn des Prinzips der Zweckbestimmung) wegfällt³. Die häufig als «schwarzes Gold des 21. Jahrhunderts» bezeichneten Daten sind, wie Tim Berners-Lee, einer der Erfinder des *World Wide Web*, sinngemäss sagte, «besser als Erdöl, denn auch wenn man sie benutzt, weitergegeben, verkauft oder ausgetauscht hat, man hat sie immer noch!».

Zudem brauchen die Maschinen dank der künstlichen, lernfähigen Intelligenz (*Deep Learning*), den Menschen immer weniger, um ihre Aufgaben auszuwählen, zu bestimmen und auszuführen, bzw. um sich zu verbessern, zu reparieren... oder serienmässig herzustellen. Es gibt «Techno-Optimisten», die mit werbewirksamem Pathos von einem «zweiten Maschinenzeitalter» sprechen.

Auch die Sharing Economy ist keine neue Erfindung. Seit Urzeiten legen menschliche Gemeinschaften seltene oder schlecht genutzte (wenn monopolisierte) Ressourcen zusammen. Die digitale Revolution erleichtert nur diesen Prozess⁴... und viele andere! Manche zögern

nicht, die neuen Technologien für Probleme verantwortlich zu machen, deren Gründe anderswo liegen, die aber schwieriger in die öffentliche Debatte zu bringen sind oder für die es schwieriger ist, Lösungen zu finden. So wurden 2011 die damals bei Jungen sehr beliebten «Blackberry»-Smartphones mit ihrem verschlüsselten Instant-Messaging-Dienst «BBM» für die Aufstände in den Londoner Vororten verantwortlich gemacht⁵. Natürlich hatten diese sozialen Unruhen ganz andere Ursachen, namentlich in der Sozialpolitik, doch es war einfacher und praktischer, die Technologie für die Ausschreitungen verantwortlich zu machen. Dasselbe gilt beim aktuellen Trend der Supermärkte, das Self-Scanning einzuführen und die Kassen mit ihren Verkäuferinnen zu ersetzen. Das wird mit dem Aufkommen der KI und Roboter in Verbindung gebracht, obwohl die Self-Scanning-Kassen nicht wirklich als «intelligent» zu bezeichnen sind. Und schliesslich sind auch die zwecks Wahlbeeinflussung geschaffenen und verbreiteten *Fake News* ein uraltes Phänomen, das die neuen Technologien vielleicht einfach sichtbarer... und (im Sinn von Klicks) messbarer machen⁶.

3. Vorteile der digitalen Revolution aus sozialdemokratischer Sicht

Arbeitswelt

Der Aufschwung der neuen Technologien bietet die Chance, um menschenwürdige Arbeit zu fördern. Die Nutzung der Technologien ermöglicht nicht nur, den Menschen zu «entautomatisieren»⁷, indem man ihn namentlich von bestimmten peniblen, zeitraubenden oder uninteressanten bzw. stumpfsinnigen Aufgaben entlastet. Das gilt für viele Tätigkeitsbereiche⁸: von John Deeres vernetzten Traktoren⁹ bis zur IBM-Software Watson, die das Mailing vereinfacht. Für viele Angestellte ist die digitale Revolution auch Synonym für gewonnene Zeit: «Alternatives économiques»¹⁰ nennt die Beispiele von Angestellten einer französischen Bank, die dank einer App, welche die Kontakte mit der Kundschaft managt, bis zu 2 Stunden pro Woche gewinnen. Ein anderes Beispiel ist die Aussage einer Versicherungsangestellten, dass die Behandlung eines Dossiers einen Monat weniger lang dauert und die Arbeitseffizienz steigt. Schliesslich können, in einer anderen französischen Bank, bis zu 50% der (einfachen) Kundenanfragen ohne menschliches Zutun geregelt werden. Die Berater können sich so (wieder) auf ihre Fachberatung, den für sie spannendsten Teil des Berufs, konzentrieren.

Zahlreiche Analysen gehen, dank den neuen digitalen Werkzeugen, auch von einer besseren Vereinbarkeit von Familie und Beruf aus¹¹.

Umwelt

Viele sehen KI als Chance für den Umweltschutz und Umgang mit natürlichen Ressourcen, namentlich Wasser¹², vor allem um die Kulturen dem Klimawandel anzupassen¹³. Die Nutzung von KI soll zudem erlauben, Biodiversität zu bestimmen und zu erhalten, den Einfluss der menschlichen Handlungen auf sie zu modellieren und die Schäden zu beheben¹⁴. Der Einsatz neuer Technologien wird auch als Mittel betrachtet, um den Mangel an Ressourcen für die Herstellung ebendieser Technologien zu bekämpfen, aber auch um ihre aktuellen physischen Grenzen zu überwinden. So könnten Grafikprozessoren (*Graphics Processing Unit*, GPU) das angekündigte Ende des «Moore'schen Gesetzes» kompensieren¹⁵.

Öffentliche Gesundheit

Viele sehen in der digitalen Revolution Chancen im Gesundheitswesen nicht nur für (zukünftige) Patienten, sondern für die Allgemeinheit¹⁶. So sollen die medizinische Analyse und Forschung, der gezielte therapeutische Einsatz, das Bestimmen von Nebenwirkungen und die Betreuung der Patienten vereinfacht werden¹⁷. Auch die Hausbetreuung von sehr betagten und/oder behinderten Personen könnte erleichtert werden, namentlich mit Sturzprävention oder der Verhinderung von Untätigkeit.

Die Gesundheitsökonomin Mascha Madörin ist überzeugt (auch wenn sie daneben ihren Pessimismus nicht verbirgt), dass die Robotertechnik die Gesundheit verbessern kann, insbesondere in der Pflegerationalisierung (im positiven Sinn des Wortes) oder im Kampf gegen den Mangel an qualifiziertem Personal¹⁸.

Öffentliche Dienstleistungen

Die neuen Technologien sollen einen besseren Zugang zu den öffentlichen Dienstleistungen ermöglichen, nicht nur im Sinn eines «physischen» Zugangs (einfach zu benutzende und ständig verfügbare virtuelle Schalter). So kann KI genutzt werden, um Anspruchsberechtigten zu helfen, ihre Formulare auszufüllen, namentlich damit ihre Dossiers komplett sind und sie keine Unterstützung verpassen, auf die sie Anrecht haben, von der sie aber nichts wissen¹⁹. Solche Fortschritte sind jedoch nur denkbar, wenn die «digitale Kluft» (s. weiter unten S. 9) verringert wird.

Der Erfolg der bewussten digitalen Politik von Estland zum Beispiel ist längst erwiesen. In diesem Land können fast alle administrativen Abläufe online erledigt werden, die Ausbildung für die neuen Technologien ist intensiv (und beginnt von klein auf), mit entsprechenden Investitionen in die Infrastrukturen. Eine solche Ausrichtung auf neue Technologien ist jedoch nicht ohne Risiko für einen Staat, vor allem wenn der Nachbar eine Grossmacht mit einer hohen Kapazität an Cyberangriffen wie Russland ist, das bereits 2007 einen massiven Angriff mit «Botnets» gegen Estland lancierte²⁰.

Wirtschaft und Konsum

Der Industrieland Schweiz, gewohnt, von technologischen Änderungen zu profitieren (wenn auch manchmal mit viel Verspätung und Kollateralschäden), könnte dank neuer Technologien als Quelle für Wachstum, Innovation, Produktivitäts- und damit Beschäftigungsgewinn gestärkt werden²¹. Das gilt jedoch nur, wenn es sich nicht um eine Innovationsphase ohne Wachstum (und damit ohne Beschäftigungswachstum) handelt: Die aktuellen technologischen Fortschritte haben einen deutlich begrenzteren Einfluss auf die Produktivität als zahlreiche grosse Innovationen vergangener Jahrzehnte. Zum Beispiel erlaubte der Übergang von der Kutsche zur Eisenbahn viel grössere Zeit- und Effizienzgewinne als die Möglichkeit, sein Ticket mit dem Smartphone zu lösen. Auch die Ausgaben für F&E liefern im Übrigen momentan deutlich weniger Return on Investment als in der Vergangenheit. Und schliesslich werden diese Produktivitätsgewinne weniger gut an die Angestellten zurückverteilt als früher, eine Tendenz, die sich mit den wachsenden Ungleichheiten, namentlich beim Kapital, noch verschärfen könnte²².

Die echte «Sharing Economy» (kollaborative Wirtschaft)²³ ermöglicht es, Ressourcen (inklusive Zeit) zusammenzulegen, nicht nur um möglichst viele davon profitieren zu lassen, sondern auch damit in Zukunft zu wenig genutzte Ressourcen häufiger genutzt werden²⁴ (insbesondere wenn man an die Investition denkt, die es braucht, um sie zu erhalten). Sie erleichtert auch intensivere soziale Kontakte (wenngleich mit dem Risiko, bis anhin ohne Gegenleistung gelieferte Dienste zu Geld zu machen). Dabei ist zu betonen, dass neben

echten Beispielen von Sharing Economy wie Wikipedia, Streetbank oder *Couch Surfing* auch zahlreiche «falsche Freunde» wie Airbnb, Uber, eBay, Upwork usw. auftauchen, die sich als Sharing Economy ausgeben, aber die gemeinsam genutzten Ressourcen zu Geld machen oder beanspruchen und davon profitieren. Zudem fördert die Sharing Economy in der Variante, in der Ressourcen zu Geld gemacht werden, die Ungleichheiten, denn nur wer besitzt, kann Ressourcen zur Verfügung stellen... und von ihrer intensiveren Nutzung profitieren²⁵.

Die digitale Revolution: ein zivilisatorischer und emanzipatorischer Prozess?

Der Aufschwung der neuen Technologien hat das Potenzial, die Weitergabe von Informationen und Wissen, aber auch die gemeinschaftliche Organisation zu revolutionieren. So gibt es Leute, die in Technologien wie P2P, Open Source oder der echten Sharing Economy einen neuen emanzipatorischen Prozess sehen, vergleichbar mit den kollektiven Erfindungen der Arbeiterbewegungen in ihren Anfängen (Gewerkschaften, Selbsthilfevereinigungen). Die neuen digitalen Werkzeuge könnten zu einer Stärkung der Gemeinschaften und ihrer Gemeinschaftshandlungen beitragen, wobei die Online-Community parallel zu oder statt den Unternehmen zum Ort der kollektiven Verhandlung werden könnte²⁶. Bauwens und Lievens²⁷ zum Beispiel sehen in den neuen Technologien eine Chance in Richtung einer relokalierten postkapitalistischen Gesellschaft, wo der Markt gezwungen wäre, sich der Logik des Gemeingutes zu beugen. Die neuen Online-Übersetzungswerkzeuge müssen noch zur Erleichterung dieser Kontakte und Selbstorganisation beitragen. Man darf jedoch nicht vergessen, dass von den neuen Möglichkeiten dezentralisierter kollektiver Organisation nicht nur Bewegungen profitieren, welche die Sozialdemokraten unterstützen bzw. zu denen sie sich bekennen: In Italien ist das M5S, die heute eine Regierungs- und Parlamentsmehrheit anführende populistische Partei, teilweise auch dank neuer Informatikwerkzeuge aus der Selbstorganisation lokaler Protestgruppchen entstanden. Neben den Fragen kollektiver Organisation könnte sich die digitale Revolution auch als zivilisatorischer Prozess manifestieren, der neue ethische Fragen aufwirft. So sagt Milad Doueïhi, der Norbert Elias paraphrasiert: «Wir [Menschen] sind heute moderne Wilde, die einem neuen zivilisatorischen Prozess unterworfen sind, dem Digitalen. (...). Unsere digitale Umwelt ist eine Art Experimentierlabor für das Zusammenleben mit dem Nicht-Menschlichen, das aber ein soziales, technisches, diskursives und wissenschaftliches Nicht-Menschliches ist. Das ist die Besonderheit des Digitalen, seiner Einzigartigkeit und seines einmaligen Status in unserer Geschichte. Es stellt den Menschen in Frage, in seinem Verhalten, seiner Identität, aber auch in seinen Werten und in der Auswahl, die er tätigen kann und über die er verfügt [insbesondere gegenüber den Algorithmen].»

4. Risiken der digitalen Revolution aus sozialdemokratischer Sicht

Arbeitswelt

Welche Folgen für die Beschäftigung?

Gerade in Bezug auf den Arbeitsmarkt werden die Folgen der digitalen Revolution intensiv diskutiert... und bleiben sehr nebulös. Pessimistische Prognosen vermischen sich mit blauäugigem Optimismus, wenn man wissen möchte, ob die neuen Technologien den Arbeitsmarkt völlig zerstören oder aber neue Stellen schaffen werden. Die meisten Analysen sind der Ansicht, dass kein massiver und umfassender Stellenabbau droht²⁸. Die Prognosen in

Bezug auf die Anzahl «bedrohter» Stellen sind sehr unterschiedlich: Einige gehen von 6 Stellen aus, die pro Roboter auf dem Arbeitsmarkt «zerstört» werden (Acemoglu); andere sprechen von 47% der Stellen, die dank KI automatisiert werden könnten und damit dem Untergang geweiht sein sollen (Frey/Osborne, auch Rifkin oder Attali, letztere wohl eher etwas karikierend), während noch anderswo von 14% (OECD) oder gar von unter 10% (Conseil d'Orientation pour l'Emploi) die Rede ist²⁹. Die ersten Beobachtungen im Feld tendieren zu einem gewissen Optimismus: In Deutschland ist man weit von einer «tödlichen Bedrohung» entfernt, wie sie unter anderem EU-Kommissar Oettinger befürchtet hatte³⁰; die Industrie schafft praktisch gleich viele neue Stellen in Zusammenhang mit der Digitalisierung, wie diese zerstört.

Stärkere globale Konkurrenz

Arbeiter in Dienstleistungsbetrieben jedoch, deren Dienste auch aus der Ferne geleistet werden können, riskieren via Plattformen eine starke unfaire Konkurrenz mit dem Weltmarkt und nicht mehr nur mit «lokalen» Konkurrenten³¹. Jede Stelle, die nicht mehr zwingend lokal verankert ist und bei der es im Wesentlichen um Informationsbearbeitung geht, kann heute leicht ausgelagert werden³². Und selbst auf lokaler Ebene können Dienstleistungen, die auf sozialen Beziehungen, Mund-zu-Mund, Nachbarschaft usw. beruhen, durch eine Plattform wie Upwork ersetzt werden, wo Handwerker ihre Dienste anbieten. Auch innerhalb eines Unternehmens wird die Konkurrenz stärker zwischen jungen, übermotivierten und gesunden Arbeitern und älteren, weniger gesunden und/oder betreuungsbedürftigen Personen. So führt die algorithmische Planung und Kontrolle von Arbeit zu Diskriminierungen der Letztgenannten³³. Dasselbe gilt für endlose Bewertungen³⁴.

Profil der bedrohten Stellen

Was das Profil möglicher bedrohter Arbeitsplätze betrifft, sind sich die Analysen einig, dass vor allem Stellen mit mittlerer Qualifikation, produktive und administrative Tätigkeiten betroffen sein könnten³⁵. Teilweise wird gar eine Umwälzung des Industriesektors befürchtet (z. B. eine neue Uhrenkrise wegen den Smartwatches), mit einer Schwächung der Gewerkschaften und der Sozialpartnerschaft sowie Verlust von Stellen mit grossem Mehrwert in wenig begünstigten Regionen wie dem Jurabogen.

Arbeitsbedingungen

Bei den Arbeitsbedingungen bringen die neuen Technologien ein gewisses Risiko der Prekarisierung zahlreicher Stellen mit sich, ebenso Risiken für die Gesundheit am Arbeitsplatz (Hyperkonnektivität, permanente Verfügbarkeit, die zu Stress und Burnout führt)³⁶. Zudem besteht die Gefahr einer Konzentration von Reichtum und Macht entlang der Wertekette in den Händen der Besitzer der Plattform (und damit der Kommunikationsnorm), was Ungleichheiten fördert³⁷. Ganz allgemein müssen die Arbeitenden der «Gig Economy» neben Unsicherheiten bei der Art ihres Arbeitsvertrages und dadurch entstehenden Lücken in den Sozialversicherungen mit schlechteren Arbeitsbedingungen und höherem Druck (insbesondere Termindruck) rechnen als in «traditionellen» Unternehmen³⁸.

Auch wenn die digitale Revolution die Schaffung neuer hochwertiger Stellen (z. B. Datenanalysten) begünstigt, fördert sie gleichzeitig die Entstehung eines neuen Proletariats von «Digitalen Sklaven» (die *Crowdworkers* von Amazons «Mechanical Turk»). Diese «Sklaven» sind auch die Arbeiter der neuen Wirtschaft, doch ihr Arbeitsplatz befindet sich nicht mehr in den komfortablen, geselligen, spielerischen und coolen Büros der Riesen des Silicon Valley, sie fahren nicht in autonomen Fahrzeugen umher... und sie kennen sich nicht,

sehen sich nie und können sich deshalb auch nicht gemeinsam organisieren (mit der bemerkenswerten Ausnahme von Turkooption)³⁹. Sie sind den Befehlen der Maschine, die sie bedienen, ausgeliefert und können ihr eigenes Know-how nicht mehr nutzen⁴⁰. Oft sind sie mit unerträglichen Inhalten konfrontiert (z. B. die Moderatoren von Gewaltvideos) und dringen in die Intimsphäre der Nutzer ein, ohne dass diese etwas davon merken⁴¹. Auf jeden Fall und wie auch immer die globalen Folgen für den Stellenmarkt sein werden, muss man sich auf eine tiefgreifende Veränderung der Arbeitswelt gefasst machen, mit einem laut SGB grossen Missbrauchspotenzial; die technologische Revolution wird mit Sicherheit Opfer fordern, deren nicht mehr gefragte Kompetenzen einen Wiedereintritt in den ersten Arbeitsmarkt verunmöglichen werden⁴².

Öffentliche Debatte / Politische Rechte

Eine beeinflusste demokratische Debatte?

Auch wenn die neuen digitalen Werkzeuge bestimmte Aspekte der Wahrnehmung politischer Rechte erleichtern (z. B. Online-Unterschriftensammlung, massive und nachhaltige Mobilisierung auch ohne Apparat im Hintergrund wie beim jüngsten Referendum gegen die Überwachung der Versicherten), bringt ihr Einsatz nicht zu vernachlässigende Risiken mit sich, die über die Zunahme der «Meinungsdemokratie» oder «Klick-/Like-Demokratie» sowie die berühmt-berüchtigten *Fake News* hinausgehen. Die GAFA könnten auf Dauer die öffentliche Debatte kontrollieren, nicht nur ihre Orte (soziale Netzwerke) und Inhalte (präventive und selektive Zensur gewisser Meinungen, die zu Recht oder zu Unrecht als extremistisch oder *Fake News* angesehen werden), sondern auch, und das ist heimtückischer, indem sie das Wording bestimmen, um die Diskussion zu lenken. Das Risiko besteht, dass das technologische Umfeld (GAFA, aber auch die Universitäten, wo ihre Technologien entstanden) die öffentliche Debatte, die über die politischen Folgen der neuen Technologien geführt werden muss, diktiert oder gar an sich reisst, indem sie wenig sinnvolle, ihnen aber entgegenkommende Begriffe setzen, wie im «Spiel» «Moral Machine» des MIT⁴³. Dieses Spiel, das helfen soll, das «Dilemma des autonomen Fahrzeugs» zu lösen, lässt die Nutzer absurde Fragen beantworten (soll bei einem akut bevorstehenden Unfall lieber eine alte Dame mit Hund oder eine Mutter mit Kinderwagen überfahren werden?), die letztlich keinen grossen Bezug zur Wirklichkeit haben. Der Beitrag zur «Inszenierung» der öffentlichen Debatte über den Einfluss der neuen Technologien, das was sie herausragend machen, schliesst das Risiko mit sein, diese Debatte letztlich zu lenken. So wird z. B. Watson (IBM) als «Augmented Intelligence» präsentiert, statt als «KI» verkauft zu werden, um den Menschen nicht Angst zu machen und ihnen Komplementarität statt eines Kampfs zwischen Mensch und Maschine zu versprechen.

Wer Gesetze zu den Folgen der neuen Technologien erlässt, muss darauf achten, sich nicht vom Grundsatz der «aus technologischer Sicht neutralen» Regeln blenden zu lassen, eine Gesetzesmethode, auf welche die Schweiz oft stolz ist. Die technologische Neutralität darf nicht mit der Neutralität des Risikos verwechselt werden⁴⁴. Die technische Neutralität verhindert, dass Regeln spezifisch für eine Technologie geschaffen werden. Aber sie verfehlt ihr Ziel, wenn sie sich nicht den Risiken einer Technologie anpasst. Nun entwickeln sich diese Risiken jedoch weiter. Man darf also die Treuekarte des Tante-Emma-Ladens nicht so behandeln wie jene der Supermarktkette, die dank Big Data extrem präzise Persönlichkeitsprofile aufgrund von an sich uninteressanten Daten erstellt, auch wenn die Technologie dieselbe ist.

Ein Steilpass für radikale Vorschläge der Rechten

Auf politischer Ebene dient die digitale Revolution, wie jeder wirtschaftliche oder soziale «Schock»⁴⁵, den herrschenden Klassen als Gelegenheit oder Vorwand, um manchmal offen, manchmal unter dem Blickwinkel des «Kampfs gegen die innovationshemmende Bürokratie» gewisse ihrer radikalsten Forderungen durchzubringen, die in einem «normalen» politischen Kontext keine Chance hätten. So wird die digitale Revolution zur neuen Rechtfertigung für viele «alte Marotten» der Rechten. Zum Beispiel ist die Denkfabrik der ultraliberalen Rechten, Avenir.Suisse der Ansicht, dass in diesen Zeiten digitaler Revolution wichtige Errungenschaften der Linken obsolet geworden seien, wie die Sozialpartnerschaft und die kollektive Verhandlung, die Arbeitszeiterfassung⁴⁶, die soziale Absicherung und der Schutz der Arbeitenden gegen falsche Abhängigkeit oder prekäre Arbeit⁴⁷. Diese Angriffe richten sich im Übrigen nicht nur gegen Angestellte, sondern auch gegen bestimmte Arbeitgebende, vor allem jene, die das Pech haben, in einer Branche tätig zu sein, die von den neuen disruptiven Akteuren (wie Airbnb oder Uber) ins Visier genommen wird. Die digitale Revolution kann auch idealer Vorwand für eine neue Privatisierungswelle öffentlicher Aufgaben sein, was für die GAFAs umso lukrativer ist, als sie über eine riesige (vor allem finanzielle) Handlungsfähigkeit verfügen, die ihnen erlaubt, rasch in jeden Markt einzudringen. Viele Ultraliberale wittern das grosse Geschäft. So will Steve Bannon, der ehemalige Berater von Donald Trump, Google mit Service-public-Aufgaben betrauen. Schliesslich wird die digitale Revolution von einigen gar dazu genutzt, das Fundament der demokratischen Debatte anzugreifen und darauf hinzuarbeiten, dass Entscheide von Behörden durch Entscheide von Algorithmen ersetzt werden.

Keine dieser Forderungen ist neu, doch die Digitalisierung der Wirtschaft genügt, um den Anschein zu erwecken, es handle sich um ein modernes und innovatives politisches Programm. Sie sollen auch den Eindruck vermitteln, dass der aktuelle Gesetzesrahmen der Innovation und dem Aufkommen der neuen Technologien nicht angepasst sei (und damit soll die Inkompetenz der demokratischen Organe gezeigt werden, die ihn eingesetzt haben), während das Geschäftsmodell einiger dieser neuen Akteure in Wirklichkeit nichts Neues an sich hat, ausser dass es auf der Nichteinhaltung der geltenden Regeln beruht. Und schliesslich ist darauf hinzuweisen, dass solche Forderungen oft unter dem Blickwinkel eines Pseudo-«Generationenkriegs» zwischen «Millennials, die mit Internet geboren sind und leben» und «alten Säcken, die nichts davon verstehen» verkauft werden.

Man muss auch sagen, dass viele Akteure der neuen Technologien stufenlos vom anarcho-libertären «Widerstand» gegen einen «exzessiv regulatorischen» Staat zum Kapitalismus in seiner klassischsten und brutalsten Form übergehen. Die GAFAs leisten durchaus Widerstand gegen den Zentralstaat, wenn dies gern gesehen wird. Es gab das Beispiel von «Apple gegen das FBI», wo die Verteidigerin der öffentlichen Freiheit dem Schnüffelstaat gegenüberstand, der das iPhone des Killers von San Bernardino entschlüsseln wollte. Es gab Microsoft, das jüngst die Auswüchse der Gesichtserkennung und den Missbrauch, den Staaten damit betreiben könnten, verurteilte, während die eigene Software breitflächig wegen ihrer rassistischen Tendenz kritisiert wurde (vgl. unten S. 14). Doch wenn es sich für ihre Geschäfte als notwendig erweist, kommen diese Unternehmen ohne zu murren den staatlichen Wünschen nach: FB entwickelt z. B. im Hinblick auf seinen Eintritt in den chinesischen Markt Mittel, um Botschaften zu blockieren. Google wiederum hat Anfang August 2018 die Absicht angekündigt, auf den Markt (den das Unternehmen 2010 verlassen hatte) zurückzukehren mit einer Suchmaschine, die von der Regierung verbotene Webseiten und Schlüsselwörter herausfiltert.

Häufig verwandeln sich die Anarcho-Libertären der ersten Stunden in brave Soldaten des oligopolistischen Kapitalismus und profilieren sich immer mehr als Anarcho-Kapitalisten, die ihren Profit maximieren⁴⁸. Oder wie es Morozov zusammenfasst: «Diese Startups können

noch so Hippie-Allüren haben, die dahinterstehenden Prozesse bleiben deswegen nicht weniger tayloristisch.»⁴⁹ Übrigens ist es interessant, die beiden «Unabhängigkeitserklärungen des Cyberspace» zu vergleichen; während die erste (1996) einen sehr libertären Unterton hatte, zielt die zweite (2018) eher darauf ab, den Bürgerwiderstand gegen die Missbräuche der GAFA zu mobilisieren.

Digitale Kluft (*Digital Divide*)

Es gibt heute keinen gleichwertigen Zugang zu den neuen Technologien, weder technisch (leistungsfähiger Zugang im ganzen Land, Leistungen, die nur online oder noch schlimmer nur auf einem aktuellen Smartphone verfügbar sind⁵⁰) noch finanziell (die meisten neuen Technologien sind teuer) und auch nicht bildungsmässig (Nutzung und Risiken)⁵¹. Informatikwerkzeuge zu beherrschen wird aber immer unerlässlicher, um am sozialen, politischen, kulturellen und wirtschaftlichen Leben teilzuhaben. Wer keinen Internetanschluss hat, riskiert nach und nach von bestimmten öffentlichen und privaten Dienstleistungen ausgeschlossen zu werden, oder die (zeitlichen oder finanziellen) Kosten einer Dienstleistung in der «realen» Welt auf sich zu nehmen (z. B. Papierrechnung mit Zuschlag). Die Tatsache, keinen (bzw. keinen leistungsfähigen) Internetzugang zu haben, hilft ebenfalls mit, die Datenbanken zu verfälschen (vgl. unten S. 13), was neue Diskriminierungen von Opfern der digitalen Kluft bewirkt⁵².

Mit der konstanten Digitalisierung der sozialen, politischen, kulturellen und wirtschaftlichen Tätigkeiten nimmt diese digitale Kluft tendenziell weiter zu... wie auch ihre negativen Folgen. Zum Beispiel korreliert die Teilnahme an der Sharing Economy mit der Höhe des Einkommens: Die höchsten Einkommen nehmen am stärksten teil, auch als Nutzniesser, obwohl diese Praktiken vor allem den tiefsten Einkommen zugutekommen sollten⁵³. Diese Kluft bedingt auch das Angebot von Online-Diensten: Es gibt viel mehr Apps für Luxusprodukte als alltägliche Konsumgüter bzw. solche für ein Publikum mit tiefer Kaufkraft (z. B. Personen mit einer Beeinträchtigung)⁵⁴.

Eine weitere digitale Kluft betrifft die Geschlechter. Sie entsteht namentlich durch die Personalstruktur der GAFA (und aller Unternehmen und Gebilden, die in den neuen Technologien tätig sind), deren Personal im Wesentlichen aus Männern besteht. Das erhöht nicht nur die Anstellungshürden für Frauen, sondern führt auch zu einer Verschärfung der Diskriminierungen, insbesondere wenn die von Männern programmierten Algorithmen hauptsächlich von Frauen wahrgenommene Probleme nicht ernst nehmen oder mit Hilfe sexistischer Klischees funktionieren (vgl. die nachfolgend unter «automatisierte Entscheide» genannten Beispiele, S. 14)⁵⁵.

Doch die digitale Kluft betrifft nicht nur Individuen: So können z. B. nur Gemeinden mit gewissen Mitteln und von einer bestimmten Grösse effizient ein «Smart City»-Verfahren durchführen... und dabei auf Augenhöhe mit dem Dienstleister verhandeln.

Privatisierung des Rechts / Straffreiheit

Der Aufschwung der neuen Technologien kann die Anwendung nationaler Gesetze wegen Problemen mit der Extraterritorialität und Lücken in der gegenseitigen internationalen Rechtshilfe viel schwieriger machen⁵⁶. So verhinderten mehrere Urteile des Bundesgerichts die Anwendung von Schweizer Recht – namentlich des Strafrechts – für Publikationen in sozialen Netzwerken, weil deren Server und Nutzerdaten sich in Ländern befinden, die nicht mit der Schweiz zusammenarbeiten oder deren nationales Recht die Anwendung des Prinzips der doppelten Strafbarkeit verhindern⁵⁷. Nur geht es nicht darum den Urheber einer Straftat zu verhaften, der aus dem Land geflüchtet ist, sondern einfach nur darum, ihn zu identifizieren.

Und wenn das unmöglich ist, profitiert er von Straffreiheit nicht, weil die Justiz ihn nicht aufgreifen kann, sondern weil sie nicht weiss, wer er ist.

Straffreiheit gibt es auch dort, wo ein Verhalten, selbst wenn es gewisse Menschen in Gefahr bringt, nicht strafbar ist und «Entschuldigungen» genügen, um sich aus der Affäre zu ziehen. Das kann zum Beispiel bei Datenverlust oder einer Vernachlässigung der Informatiksicherheit der Fall sein, wie bei FB, das im Juli 2018 irrtümlicherweise Hunderte von Kontakten in seiner Messenger-App deblockierte, was Belästigern ermöglichte, erneut mit ihren Opfern in Kontakt zu treten⁵⁸.

Das immer grössere Gewicht der GAFAs führt auch zu einer Privatisierung des Rechts⁵⁹: Diese Firmen legen ihre eigenen Regeln fest und wenden sie an, egal ob sie dem geltenden Recht, in dem sie ihre Tätigkeiten entfalten, entsprechen oder nicht. Es ist nicht einmal sicher, ob sie einem irgendwo geltenden Recht entsprechen. So hat der Guardian die internen Richtlinien von Facebook für die Moderation der Publikationen enthüllt. Diese Richtlinien schreiben zum Beispiel die Löschung absolut legaler Publikationen in der Schweiz vor, während sie verhindern, dass andere, offensichtlich illegale wie die Darstellung von Kindsmisshandlungen, zurückgezogen werden⁶⁰. Jüngst hat der FB-Gründer Mark Zuckerberg erklärt, dass sein Netzwerk die Leugnung des Holocaust nicht blockiere, obwohl das in mehreren Ländern klar illegal ist, mit der Begründung, es handle sich nicht um «Fake News», da die Leugner von ihren Theorien überzeugt seien!⁶¹

Der Trend kann auch durch staatliche Regeln wie das deutsche *Netzwerkdurchsetzungsgesetz* verstärkt werden, das unter Androhung hoher Bussen vorschreibt, sehr rasch jede «offensichtlich ungesetzliche» Publikation zu löschen, ohne dass jedoch die Illegalität der fraglichen Publikation durch eine rechtliche Instanz geklärt wird.

Die digitale Revolution bringt auch ein Risiko privater Justiz mit sich. Das kann der Fall sein, wenn es keinen Schutz mehr gegen einen populistischen Shitstorm in den sozialen Medien ohne Respektierung der Verteidigungsregeln und mit dem hohen Risiko eines «sozialen Todes» (vgl. unten S. 18) durch digitale Lynchjustiz gibt. In gewissen Fällen kann man gar von «Privatarmeen» im Dienst von Firmen oder Personen sprechen, die bereit sind, digitale Grossangriffe als Vergeltung gegen Kritiken zu starten.⁶² Eine Privatisierung der Justiz besteht auch dort, wo private Organisationen mit ideellem Zweck, selbst wenn sie gute Absichten haben, nicht nur die öffentlichen Entscheide kritisieren, sondern digitale Angriffe starten, um sie aufheben zu lassen (z. B. der Angriff auf PostFinance durch Anonymous als Vergeltung gegen die Schliessung des Postkontos von Julian Assange⁶³).

Das Gewicht der GAFAs, aber auch grosser Firmen ganz allgemein, verschärft das Risiko einer generellen Nichteinhaltung des Rechts, denn dank ihrer Grösse und ihres Reichtums können sie allfällige strafrechtliche, administrative und zivile Sanktionen problemlos verschmerzen. Im Schweizer Recht sind nur wenige Bussen mit abschreckenden Beträgen vorgesehen⁶⁴, und selbst wenn sie es theoretisch sind (z. B. die Sanktionen in Art. 49a des KG), machen sie den ebenso reichen wie riesigen Unternehmen kaum Angst. Unser Recht sieht auch keine Gruppenhandlungen (*Class Action*) vor, die geschädigten Personen eine Sammelklage ermöglichen würden, wo wegen der tiefen Entschädigungen für jede Person Einzelklagen kaum Sinn machen. Trotz fehlender wirklich abschreckender Sanktionen oder der Möglichkeit, die Anwendung von Schweizer Recht aus Gründen der Extraterritorialität zu umgehen, haben die GAFAs jedoch die Tendenz, die rechtskräftigen Entscheide der Justiz zu respektieren, wie das namentlich beim BG-Entscheid zu «Google Street View» der Fall war.

Persönliche und öffentliche Freiheiten

Totale Kontrolle unseres Daseins durch die GAFA?

Der Aufschwung der neuen Technologien könnte zu einer schrittweisen, unbewussten und passiven Aufgabe der Freiheiten führen. Die GAFA übernehmen nach und nach die Kontrolle über viele, wenn nicht gar alle, unserer Lebensbereiche. Kerdellant sagt über Google: «Die Maschine erfindet nichts, "stiehlt" uns nichts, sie begnügt sich damit, zu sammeln und allem, was sie in den ihr zur Verfügung stehenden Quellen gesammelt hat, einen Sinn zu geben: den Inhalt unserer Mails für alle, die ein Gmail-Konto haben (Google versichert, diese Inhalte nicht mehr zu lesen), unsere Suchanfragen, unsere Navigations-History (Google Chrome), die Bilder (Google Photos), unsere Vorlieben für gewisse Arten von Videos, unsere Weckzeit oder die Aktualisierung unseres Facebook-Profiles (mit Android auf dem Smartphone), unsere Fahrten (Google Maps – AdA: neu für Unternehmen und Institutionen gebührenpflichtig!!!), wie wir Zeit verbringen (Google Now), der Inhalt geteilter Dateien (Google Docs), unsere Notizen (Google Drive), unsere Einkäufe (Android Pay). Jeder neue Dienst erhöht die intimen Kenntnisse, die Google von uns hat, denn das Gedächtnis der Maschine ist unendlich». Und Google (durch seinen CEO Eric Schmidt, Berlin 2010) dementiert nicht: «Wir wissen wo du bist, wir wissen wo du warst, wir wissen mehr oder weniger, worüber du nachdenkst.» Schliesslich soll daran erinnert werden, dass eine freiheitsfeindliche Nutzung der neuen Technologien nicht nur privaten Firmen vorbehalten ist, sondern auch die – legale oder illegale – Massenüberwachung durch Staaten rigoros vereinfachen kann, insbesondere via Nachrichtendienste. Die neuen Technologien erlauben zudem den repressiven Staaten nicht nur, ihre Bevölkerung besser zu kontrollieren, sondern auch deren Verhalten zu beeinflussen oder gar zu diktieren, wie beim Ratingsystem des «Sozialverhaltens» der Bürger in der Volksrepublik China.

Vom Anreiz zum Zwang

Natürlich ist niemand gezwungen, die neuen Technologien zu nutzen bzw. sie alle zu nutzen. Doch ihre extrem weite, um nicht zu sagen universelle Verbreitung kann auf Dauer zu einem Zwang führen, sie zu akzeptieren... und sich ihnen zu beugen. Das beginnt bei Anreizen und Rabatten (KVG-Prämienrabatt bei Nutzung des QS, Autoversicherungsrabatt bei Nutzung der *Dashcam*), danach kommen die Anordnungen, zum Beispiel des Arbeitgebers (Pflicht, ein internes Gesundheitsprogramm mit QS zu nutzen), dann eine faktische Pflicht, wenn der Rabatt für die ersten Kunden, die eine bestimmte Technologie nutzen, sich in einen Malus für jene, die sich ihr verweigern, verwandelt.⁶⁵

Zudem kann der Einsatz neuer Technologien durch die öffentlichen Behörden zum Verschreiben bestimmter Verhaltensweisen führen, oder auch zur Schaffung neuer sozialer Normen⁶⁶, denen sich die Leute aufgrund der Algorithmen zwingend anpassen müssen: Das geht von der absoluten Pflicht einer (im Übrigen sinnvollen) Gesetzesnorm, wenn ein «intelligentes» Fahrzeug bei nicht angegurtem Chauffeur sich weigert zu starten, bis zur faktischen Pflicht, ein bestimmtes Verhalten anzunehmen, um nicht «suspekt» zu erscheinen, zum Beispiel wenn ein Algorithmus, der mittels Bildauswertung der Videokamera ein «zweifelhaftes Verhalten» von Passagieren an einem Flughafen «aufspürt»⁶⁷, diese damit zwingt – ohne dass es irgendwo vorgeschrieben wäre – ruhig zu gehen, keine brusken Bewegungen zu machen, vorhersehbare Wege zu nehmen usw. Diese Diktatur der Algorithmen kann sich mit der Zunahme vernetzter Geräte in verschiedenen Formen zeigen: vom smarten Gurt «Belty», der zu mehr Aktivität zwingt (z. B. mehr Treppensteigen) über den smarten Spiegel «HiMirror», der die Falten analysiert, bis zum Präservativ «i.Con», das alle Daten einer sexuellen Beziehung entschlüsselt. Das meiste davon bringt uns im Moment

noch zum Lachen... bis dann deren Verbreitung zu neuen sozialen Normen führt, die auf breiter Ebene zur Anwendung kommen.

Schliesslich wird es in Zeiten von Big Data, die uns alle aufgrund irgendeines Kriteriums kategorisieren können, immer schwieriger, von individueller Verantwortung zu sprechen⁶⁸.

Das Ende der Verantwortung?

Doch die individuelle Freiheit wird nicht nur durch das bedroht, was sie behindert, sondern auch durch den schrittweisen Abbau ihres Pendants, der Verantwortung (zumindest der zivilen). Zahlreiche Trends der digitalen Revolution tendieren dazu, die Verantwortung völlig auszulöschen. Nun ist aber die Verantwortung bei einer unlauteren Handlung der zwingende Gegenpart der persönlichen Freiheit. Den Schaden zu übernehmen, den man den rechtlichen Gütern anderer zufügt, ist die Kehrseite der Medaille und die unerlässliche Ergänzung zur Freiheit; ebenso ein unabdingbares Instrument, um den sozialen Frieden zu sichern⁶⁹.

Wenn nun ein Algorithmus entscheidet, so verschwindet die Verantwortung⁷⁰. Das ist auch der Fall, wenn niemand Verantwortung übernehmen will, zum Beispiel bei einer Plattform wie Uber, die sich als «einfache Vermittlerin» zwischen Kunde und Dienstleistungsanbieter (bzw. allfälliger Dritter) sieht und nicht davon wissen will, was dem einen oder andern wegen eines dem einen oder andern zuzuschreibenden Fehlers passieren kann⁷¹. Das gilt auch, wenn es unmöglich wird, eine Firma zu kontaktieren, deren Dienst zu grossen ungeplanten Beeinträchtigungen führt (wie ein GPS-Dienst, der den Verkehr durch ein Wohngebiet lotst, weil es eine Abkürzung ist). Oder wenn der Schaden durch einen Roboter verursacht wird, dessen KI lernfähig ist, ein Fehler, der nur schwer einer natürlichen oder juristischen Person angelastet werden kann, die ihn beheben könnte, weil der Hersteller der Ansicht ist, dass die zum Schaden führende Handlung in der ursprünglichen Programmierung der KI nicht enthalten war, und der Nutzer des Roboters argumentiert, dass es Aufgabe des Herstellers gewesen wäre, die KI so zu programmieren, dass der Schaden nicht eintritt.

Selbst wenn es sich nicht zwingend um eine Abkehr von den individuellen und kollektiven Freiheiten handelt: Einen immer grösseren Teil unseres Daseins den neuen Technologien anzuvertrauen, um sich das Leben zu erleichtern, könnte mehr negative Folgen als erhofft haben, namentlich für unsere Fähigkeiten, unseren Lebensstil selber zu wählen und eigene Entscheide zu treffen⁷². Gemäss Nicholas Carr⁷³, Essayist und Experte für neue Technologien, «macht die Hypertechnologie unsere Leben ärmer, denn sie treibt uns dazu, unsere eigenen Talente und Kompetenzen zu vernachlässigen». Carr warnt deutlich vor dem Risiko, dass die Fähigkeit, moralische Urteile zu fällen, verloren gehen könnte.

Auch ohne zu diesem Schluss zu kommen, ist klar, dass der allgemeine Einsatz der Technologie das Leben risikoreicher machen kann: Beim Air-France-Crash 2009 übernahm der Autopilot das Zepter und die Piloten konnten die Lage manuell nicht mehr bereinigen. Wer blind der Technologie folgt, namentlich den Algorithmen, und sei es auch nur aus Gründen der Routine, des Komforts oder der Effizienz, verliert letztlich seine Autonomie. So verstarb im Oktober 2014 ein Ebola-Patient in Dallas an den Folgen von Diagnosefehlern und schlecht oder gar nicht gestellten Fragen des Pflegepersonals, welches «das vorgesehene Verfahren befolgte»⁷⁴. Allerdings ist dieses Risiko nicht zwingend an die digitale Revolution gebunden, es besteht auch mit jedem nicht-digitalen Algorithmus wie Formularen, Checklisten und anderen Rezepten.

Automatisierte Entscheide

Eines der grössten Risiken im Bereich der persönlichen Freiheit beruht auf dem Aufkommen staatlicher oder privater automatisierter Entscheide. Die Algorithmen «helfen» den Entscheidern immer mehr, Entscheide zu treffen, oder treffen sie gleich selber. Nun sind wir

aber nicht alle gleich vor den Algorithmen, und die Parteilichkeit hat reale Folgen für unser Leben⁷⁵. Zudem entscheidet ein blind den «Empfehlungen» des Algorithmus folgender «Entscheider» nicht, sondern er gehorcht⁷⁶.

Zu den eindrücklichsten Beispielen gehört die Software der «prädiktiven Polizei» wie PRECOBS⁷⁷, die namentlich in den Kantonen Aargau und Baselland sowie in der Stadt Zürich zum Einsatz kommt. Die einst in der Science-Fiction – wie in der Novelle «The Minority Report» (1956) von Philip K. Dick – auftauchenden Programme können «vorhersagen», wo und wann gewisse Delikte stattfinden werden, namentlich Einbrüche, was den Ordnungskräften erlaubt, rechtzeitig, manchmal gar präventiv, einzugreifen. Und wenn die KI von den Ordnungskräften genutzt werden kann, so machen das natürlich auch die Kriminellen, um ihre Beute zu identifizieren, zu überwachen, Profile zu erstellen oder sich damit vertraut zu machen⁷⁸.

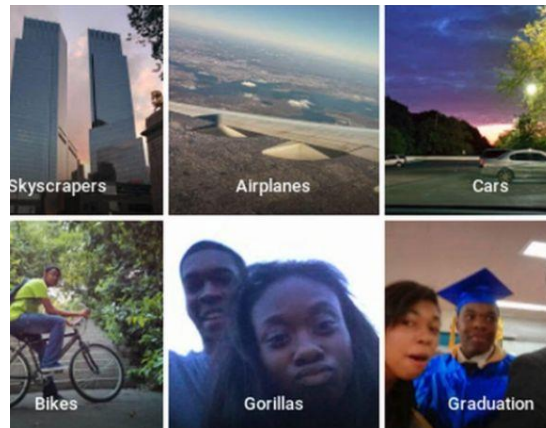
Das Fiasko der Software «Parcoursup» für die Zuweisung von Uni-Ausbildungsplätzen in Frankreich (deren Quellcode grossteils öffentlich ist) zeigt deutlich die Risiken, wenn man Algorithmen statt Menschen beauftragt, Entscheide zu treffen, selbst wenn es darum geht, effizienter oder «objektiver» zu sein (vgl. dazu weiter unten S. 18). Die erwartete Zuverlässigkeit stellte sich nicht ein: Die Hälfte der Kandidaten erhielt in der ersten Auswahlrunde keinen Platz (während das Los des früheren, zweifellos keineswegs perfekten⁷⁹ Systems nur gerade... 1% der Kandidaten ausschloss). Im Übrigen scheint der Algorithmus Diskriminierungen zu reproduzieren, denn die Schüler weniger bekannter Institute (namentlich aus so genannt «schwierigen» Quartieren) haben mehr Mühe einen Platz zu finden, selbst mit hervorragenden Noten⁸⁰. Das scheint sich bei der Zuteilung von Stipendien zu bestätigen⁸¹.

«Parcoursup» ist keineswegs das einzige Beispiel einer Diskriminierung aufgrund von automatisierten Entscheiden. Hier ein paar weitere:

- Infolge des vorherrschenden Rassismus werden die schwarzen Chauffeure bei Uber weniger gut bewertet, erhalten also weniger Fahrten. Dasselbe geschieht bei Airbnb, das empfiehlt, sein Foto auf das Wohnungsprofil zu stellen, die man vermieten will. Die Folge: In der Stadt New York können Nicht-Afroamerikaner von ihren Gästen eine um 12% teurere Miete verlangen.
- Ein Auswahlfilter von Bewerbern einer Firma, deren Personal sich vor allem aus weissen Männern mit MBA zusammensetzt, wird nur diese Profile auswählen und damit die Diskriminierungen weiter verschärfen. Es gab auch Google-Stellenangebote für Frauen... mit tieferem Lohn⁸².
- Die in den USA eingesetzte Software, die strafrechtliche Rückfälle voraussagt (einzelne Programme wie ROS werden auch in der Schweiz genutzt⁸³), benachteiligt ethnische Minderheiten, die, weil ärmer, mehr von Kriminalität betroffen sind.
- Siri (Apple), vorwiegend von Personen männlichen Geschlechts programmiert, macht sich über eine Frau lustig, die Opfer einer Vergewaltigung wird und fragt, was sie tun solle und wo sie Hilfe finde⁸⁴.
- Die Suchmaschine von Google ist voller sexistischer Klischees, zum Beispiel wenn sie bei einer Suche nach wenig prestigeträchtigen Stellen nur Frauenbilder zeigt oder eine Aufgabenteilung nach patriarchalischem Modell suggeriert, wenn man eingibt «Frauen sollten... »⁸⁵.
- Bildbearbeitungsprogramme wie FaceApp oder Google Photos, die Fotos von farbigen Personen als «Gorillas» klassieren oder die Haut aufhellen, damit die fragliche Person «sexy» aussieht⁸⁶.
- Die Gesichtserkennungssoftware «Face API» von Microsoft musste (gemäss Herausgeber mit Erfolg) korrigiert werden, nachdem mehr als 93% der Fehler

Gesichter mit dunklem Teint betrafen, wegen einer Programmierungs-Datenbank, die vor allem weisse Männer enthielt⁸⁷.

- Streetbump (von der Stadt Boston genutzt): Die GPS-Daten lassen erkennen, ob die Trottoirs abgenutzt sind, wenn die Leute stolpern. Doch da die weniger Reichen weniger Smartphones haben und weniger verbunden sind, werden die Trottoirs ihrer Quartiere weniger oft repariert...



Ein Entscheid von Algorithmen beruht immer auf Daten, die niemals neutral oder objektiv sein können. Programmierungsdaten sind immer verfälscht, denn es handelt sich um soziale und historische Konstruktionen⁸⁸. Sie sind das Ergebnis von vorgefassten Kollektivurteilen. Sie hängen auch von der Lokalisierung der Sensoren ab. Automatisierte Entscheide haben deshalb ein hohes «Ansteckungsrisiko»: Wenn z. B. zahlreiche Bewohner Ihres Quartiers schlechte Zahler sind, so werden Sie vom Algorithmus auch als solcher eingeschätzt, weil er eine Korrelation «Wohnort – Bonität» herstellt⁸⁹.

Was im Übrigen diese neue algorithmische Rationalität interessiert, ist, uns bis in die kleinsten Details zu kennen, ohne uns vorher angehört zu haben, da Motivationen und Begründungen von Individuen überhaupt keine Rolle mehr spielen⁹⁰.

Privatsphäre / Schutz der persönlichen Daten

Die digitale Revolution, insbesondere *Big Data* bringt offensichtliche und bekannte Risiken für die Privatsphäre mit sich. Langsam merken das auch die Behörden, selbst wenn die Verspätung riesig ist. Villani zum Beispiel sagt (und hat vermutlich Recht), dass die GAFA, wenn es die DSGVO schon vor 20 Jahren gegeben hätte, den europäischen Markt nicht so einfach hätten durchdringen können und die Konkurrenz stärker gewesen wäre⁹¹. Nun ist aber der Datenschutz keine Antitrust-Massnahme gegen die GAFA, sondern ein Mittel, um die öffentlichen Freiheiten zu schützen. Der «Mehrwert» des Rechts auf Datenschutz im Vergleich zum Schutz des Privatlebens liegt genau darin, dass zu dessen Ziel auch ein Abbau der Macht- und Informations-Asymmetrien zwischen den Nutzern der Dienste und jenen, die die Daten sammeln, gehört⁹².

Auch wenn die Sensibilisierung von öffentlichen Behörden, Firmen und Personen (langsam) zunimmt, sind Verhaltensweisen, die den Datenschutz verletzen, noch immer häufig, selbst wenn sie durch vorsichtige und gewissenhafte Verarbeitungsbeauftragte erfolgen. So wird das Risiko der Re-Identifikation durch Datenverknüpfung von Daten noch immer breit unterschätzt, während zahlreiche Dateien, die anonym sein sollten und deren Daten in öffentlichem Interesse (z. B. wissenschaftliche Forschung) gesammelt wurden, die Persönlichkeit der Personen, welche die Daten geliefert haben, keineswegs schützen⁹³. Zum Beispiel können Transaktionen über drei Monate von 1,1 Millionen «anonymisierten»

Kreditkarten mit gerade mal 4 räumlich-zeitlichen Daten zu 90% identifiziert werden⁹⁴. Und in keinem Fall ermöglicht die Online-Anonymität, eine Charakterisierung des Verhaltens von Individuen zu verhindern, genauso wenig wie eine prädiktive Analyse dieses Verhaltens⁹⁵. Ein grosses Risiko der digitalen Revolution versteckt sich hinter dem «Ich habe nichts zu verbergen»-Argument, das ein Grossteil der Bevölkerung (der Autor dieses Dokuments inbegriffen) vorschreibt, um den Schutz der persönlichen Daten auf die leichte Schulter zu nehmen. In einer Welt, in der die einzige Art, sensible Daten zu erhalten (z. B. politische oder religiöse Meinungen, Gesundheitszustand usw.) darin bestand, diese Daten explizit zu übermitteln, konnte man legitimerweise davon ausgehen, dass niemand sie kannte, solange man keine intimen Details lieferte. Doch diese alte Welt gibt es nicht mehr. In der Ära von «Big Data», wo es möglich ist, mit Hilfe von an sich harmlosen Daten (z. B. eine Einkaufsstatistik) extrem detaillierte Persönlichkeitsprofile zu erstellen, kann man nicht mehr einfach annehmen, dass keine Drittperson diese sensiblen Daten besitzt⁹⁶. Solange man zudem nicht weiss, was der/diejenige sucht, der /die eben sucht, kann man unmöglich behaupten, man habe «nichts zu verbergen», denn einzig aus Sicht der suchenden Person kann man bestimmen, was man «verbergen» sollte. Diese Tendenz kann auch zu einer Aufhebung des Rechts auf Privatsphäre führen, das von Manchen als unnötig angesehen wird, denn «wer sein Leben in den sozialen Netzwerken erzählt, hat de facto kein Privatleben mehr». Nun umfasst aber das Recht auf Privatsphäre nicht nur das Recht, verborgen zu bleiben, sondern auch jenes der Selbstbestimmung im Bereich der Information (vgl. weiter unten S. 29), also das Recht selber zu entscheiden, was öffentlich werden soll (das was – wenn manchmal auch eher unüberlegt – derjenige macht, der sich entscheidet, bestimmte intime Details im Netz preiszugeben).

Allgemein bringt die digitale Revolution das Risiko mit sich, aus der Privatsphäre ein Recht zu machen, das man erwerben muss oder «das man sich leisten kann»⁹⁷. Gemäss dem Zukunftsforscher Gerd Leonhard wird «offline sein zu einem Luxus, der weniger als 1% der Bevölkerung zugänglich sein wird»⁹⁸.

Umwelt / Energie

Gewisse Analysen prognostizieren, dass bis 2040 die Nachfrage nach Lagerkapazität die weltweit verfügbare Produktion von Silicium übersteigen könnte. Der Energieverbrauch des Digitalen nimmt stark zu, ebenso sein Anteil an der Produktion von Treibhausgas⁹⁹. «Gemäss Alex Wissner-Gross, Physiker an der Universität Harvard, sollen zwei Google-Suchanfragen gleich viel CO₂ verbrauchen wie eine Tasse heisser Tee. Den Arbeiten des Wissenschaftlers zufolge verursachen zwei Google-Anfragen 14 g CO₂-Ausstoss, also fast so viel wie ein elektrischer Wasserkocher (15 g). (...) Nach einem neuen Bericht des Analysezentrum Gartner verantwortet die Informatikindustrie allein 2 % der Treibhausgasemissionen, noch vor der Luftfahrtindustrie. Die simple Nutzung eines Computers verbraucht zwischen 40 g und 80 g CO₂ pro Stunde, erläutert John Buckley, Leiter von Carbonfootprint, einem britischen Expertenbüro für Umweltfragen. Die Abfrage einer einfachen Webseite verbraucht allein 0,02 Gramm CO₂ pro Sekunde, mit einer Verzehnfachung bei einer Seite mit komplexen Bildern oder Videos (0,2 Gramm). Noch überraschender: Die Erhaltung eines Avatar-Lebens im Virtual-Reality-Spiel Second Life während eines Jahres soll ebenso viel Energie verbrauchen wie ein durchschnittlicher Brasilianer, nämlich 1 752 Kilowattstunden.»¹⁰⁰. Ein anderes Beispiel sind die Kryptowährungen: Island hat «dank» seines frischen Klimas (wodurch die Server zu tieferen Kosten gekühlt werden können) und dem sehr tiefen Energiepreis zahlreiche «Bitcoin-Schürfer» angezogen. 2018 soll der Energieverbrauch des Schürfens jenen aller Haushalte im Land übertreffen. Zudem haben diese Tätigkeiten praktisch keine Stellen oder Steuereinnahmen geschaffen¹⁰¹.

Die Vervielfachung der Kommunikationskanäle (M2M, Internet der Dinge) kann zur Sättigung der Infrastrukturen (mit und ohne Kabel) führen, aber auch zu ihrer Vervielfachung. Gemäss Bradley et al. wird es 2050 50 Milliarden vernetzte Dinge geben, man muss also die Antennen vervielfachen, namentlich um neue Übermittlungstechnologien einzuführen: Da weniger Informationen übertragen werden müssen, brauchen viele Kommunikationen zwischen Dingen nicht so leistungsfähige Kanäle wie z. B. 4G. Die gleiche Überlegung gilt für die neuen, in Sachen Datentransfer «gefrässigen» Onlinedienste: In den USA zum Beispiel braucht Netflix in den Spitzenzeiten ein Drittel der Bandbreite! Schliesslich könnten die mit der breiten Einführung autonomer Fahrzeuge erwarteten Fortschritte im Verkehrsmanagement paradoxerweise zu einer Zunahme des Verkehrs führen, weil die Nutzer auf den öffentlichen Verkehr verzichten würden, um stattdessen ein robotisiertes Kleinauto zu nehmen¹⁰².

Wirtschaft/Konsum

Konzentration der Akteure

Obwohl sie sich als liberal und Verfechter der Marktwirtschaft geben, ist das Ziel der GAFA nichts weniger, als Oligopole oder gar Monopole zu schaffen¹⁰³. Zumindest ist das die Ansicht eines der Leiter dieser Unternehmen, des PayPal-Gründers Peter Thiel. Diese riesigen Firmen profitieren in erster Linie von ihrer Grösse (und der Grösse ihrer Liquiditätsreserven), dank der sie ohne Probleme innovativere, etablierte Konkurrenten aufkaufen können (wie WhatsApp oder Instagram, die von FB übernommen wurden) oder solche, die kurz vor dem Durchbruch stehen, um jede Konkurrenz im Keim zu ersticken. Je grösser ein Unternehmen ist, desto mehr kann es investieren, um seine Algorithmen zu verbessern, neue Dienste einzuführen und damit in anderen Branchen Fuss zu fassen und das eigene Monopol auszuweiten. Google z. B. setzt auf den Service public im Stellenmarkt – Google for Jobs, die Gesundheit – Integration der Software in einen Operationsroboter Johnson & Johnson – die Alzheimerforschung, die Optik – vernetzte und intelligente Kontaktlinsen, Kriegsmaterial – Kampfdrohnen... Vergleichbare Situation (wenn auch im kleineren Rahmen): Die Swisscom, die beim «Service public» mit Lösungen wie *Smart Cities* für die Gemeinden mitarbeitet... und dies ausnutzt, um Daten für eigene Zwecke zu sammeln.

Diese Firmen profitieren auch von den «Netzwerk-Effekten»: Wer schon viele Kunden und eine kritische Grösse hat, für den ist es sehr rentabel, einen neuen Dienst zu lancieren (und dabei allenfalls aufkommende Anbieter aufzukaufen)¹⁰⁴. Diese Netzwerk-Effekte verstärken den «Alles dem Sieger»-Trend (*The winner takes it all*): Die Technologie, die sich auf dem Markt durchsetzt, wird zum Markt selber und schliesst jede Konkurrenz aus¹⁰⁵. Dazu trägt auch die, wie sie Villani nennt, API-sierung der Wirtschaft bei, das heisst die Möglichkeit, auf Basis der Schnittstellen, die von den Plattformen zur Verfügung gestellt werden, Innovation zu betreiben, was wiederum die Macht der Plattformen stärkt, während es die Entwickler der externen Dienstleistungen sind, die investieren, dabei aber gebunden bleiben¹⁰⁶.

Eine weitere Folge dieser Konzentration ist, dass andere Dienstleistungsanbieter rasch von den Diensten der Netzriesen (booking.com/Tripadvisor usw. bei den Hotels, Facebook/Twitter bei den Medien) abhängig werden, was diesen erlaubt, ihre Monopole auf neue Branchen auszuweiten, ohne dafür einen Rappen zu investieren. Solche Monopol-Situationen können katastrophale Folgen für eine ganze Branche haben, wie die Algorithmus-Änderung von FB zeigt, um die Beiträge von «Freunden» zu Lasten von jenen der Medien zu privilegieren. Dies brachte mehrere «Pure Players» wie z. B. brut.fr in Schwierigkeiten, die ja nicht alle Clickbaits wie z.B. Buzzfeed France sind. Die Inhalte dieser seriösen Medien sind auf FB weniger sichtbar geworden und werden also weniger geteilt¹⁰⁷. Die katastrophalen Folgen zeigen sich auch, wenn die Plattform ihre beherrschende Stellung missbraucht, um

vertragliche Knebel-Klauseln durchzusetzen, wie booking.com, das seinen gebundenen Kunden untersagt, ihren Direktkunden tiefere Preise anzubieten.

Schliesslich ist zu betonen, dass die Konzentration der Akteure nicht nur Firmen betrifft: So kontrollieren inzwischen weniger als 20 «Schürfer» die *Blockchain* des Bitcoin¹⁰⁸ ... eine Kryptowährung, die frei (oder gar libertär) und dezentralisiert sein wollte... Airbnb, in seinen Anfängen einer der Vorreiter der echten Sharing Economy, kann sich der Marktkonzentration auch nicht entziehen: In der Schweiz machen die professionellen Übernachtungsanbieter mit mehr als zehn Mietobjekten bereits 19% der Vermietungen aus (gegenüber 5% 2015), und der grösste Anbieter verwaltet... 184 Wohnungen¹⁰⁹. Damit sind wir weit weg von der Idee der Einzelpersonen, die sich gegenseitig Dienste anbieten!

Unlauterer Wettbewerb

Es ist allgemein bekannt, dass die digitale Revolution den unlauteren Wettbewerb erleichtert, wenn «disruptive» neue Akteure auf einen Markt drängen, deren Geschäftsmodell auf einer völligen oder teilweisen Missachtung der für ihre Konkurrenten geltenden Regeln beruht (z. B. Uber und das Arbeitsrecht, die Sozialversicherungen sowie die Regeln für den Personentransport). Einer der Slogans, die im Silicon Valley in Mode sind, lautet denn auch: «*Move fast and break things*». Obwohl der Trend an sich nicht neu ist, birgt er doch im Gegensatz zum «klassischen» Unterbieten die Gefahr in sich, dass er bei der Rechten und im Arbeitgeberrmilieu gern gesehen ist; einige sind geblendet vom Disruptiven und der «neuen innovativen Wirtschaft 4.0, die die Welt verändern wird», andere sehen darin eine Chance (endlich) radikale Vorschläge für Sozialabbau durchzubringen (vgl. S. 8). Die GAFAs und weitere Internetriesen profitieren auch von ihrer Grösse und Finanzmacht, um sich mit der Subventionierung ihrer eigenen Dienstleistungen in einem Markt zu etablieren (z. B. Amazon, das bei einem Eintritt in einen Markt gratis liefert), oder um sie so lange verlustreich anzubieten, bis die Konkurrenz ausgeschaltet ist (Uber, das immer noch nicht rentabel ist). Doch der unlautere Wettbewerb kann weitere Formen annehmen, die durch die Digitalisierung der Wirtschaft stark erleichtert werden. Es gibt z. B. das «*Review Bombing*» (bzw. die simple Drohung, es auszulösen), das heisst die Bombardierung mit schlechten Bewertungen in den sozialen Netzwerken bzw. den spezialisierten Webseiten¹¹⁰. Dennoch sind Online-Bewertungen für Geschäfte und Konsumenten eher eine Chance: Die Studien zeigen, dass es tendenziell mehr positive als negative Kommentare gibt¹¹¹. Das Funktionieren der Märkte kann schliesslich durch gefälschte Bonitätsprofile gestört werden, die den fälschlicherweise als insolvent hingestellten Personen schweren Schaden zufügen... ebenso ihren potenziellen Geschäftspartnern, die wegen der Falschinformationen möglicherweise Chancen verpassen¹¹².

Angesichts des Volumens, das die allgemeinen Nutzungsbedingungen der meisten Online-Dienste annehmen, kann man zudem immer weniger von freien Märkten sprechen, wo Dienstleistungsnehmer und -anbieter auf Augenhöhe miteinander verhandeln. Wer immer die wichtigsten Online-Dienste nutzen will, hat keine andere Wahl als viele seiner Freiheiten aufzugeben und knebelartige Bedingungen zu akzeptieren, ohne Zeit zu haben, die Tausenden von Seiten zu lesen, und ohne auch nur die kleinste Alternative zu haben, da eine solche wegen den Monopolen der Netzriesen oft gar nicht besteht. Und selbst wenn es einen Konkurrenten gibt, dann fordert dieser selber auch die Zustimmung zu ähnlichen allgemeinen Geschäftsbedingungen.

Ausserdem könnte die digitale Revolution die Entstehung von Kartellen fördern, gegen welche die aktuelle Gesetzgebung machtlos wäre, dank dem Einsatz von Algorithmen, die eine mit niemandem abgesprochene Preis-Parallelität schaffen¹¹³.

Neue Spekulationsrisiken

Schliesslich kann die digitale Revolution jedes Mal, wenn neue sehr gefragte Produkte auf den Markt kommen, Spekulationsblasen (Domainnamen, Kryptowährungen usw.) bilden. Das ist umso beunruhigender, als die Technologiefirmen der USA der 2010er Jahre genau wie jene, die den 2000er Jahren mit Immobilien spekulierten, versuchen Reichtum zu schaffen, indem sie auf die Wertsteigerung ihres Vermögens setzen, während die so genannte «reale» Wirtschaft in Schwierigkeiten geriet¹¹⁴.

Gesundheit und persönliche bzw. öffentliche Sicherheit

Neben den bereits bekannten (und ausführlich beschriebenen) Risiken der Hyperkonnektivität und ständigen Verfügbarkeit ist leider klar, dass die digitale Revolution nicht ohne Folgen für die öffentliche Gesundheit bleibt. Zum Beispiel hat in den USA die Depressions- und Suizidrate zugenommen, im Wesentlichen wegen den sozialen Netzwerken¹¹⁵.

Abgesehen von persönlichen Gesundheitsproblemen (ob heilbar oder nicht) bringen die neuen Technologien, insbesondere die sozialen Netzwerke, auch ein neues Risiko mit sich: den «sozialen Tod», das heisst, dass der eigene Ruf innert Stunden durch die unaufhaltsame Verbreitung von Informationen, Bildern oder Zitaten (sowie der Kommentare der Internetnutzer) nachhaltig ruiniert wird, egal ob wahr oder nicht; sie werden unauslöschlich und weiten sich häufig noch aus¹¹⁶. Dieses Phänomen des «sozialen Todes» (das zum Tod *tout court* führen kann)¹¹⁷ kann auch durch einen (koordinierten) «Angriff» (oder eine grosse Nachlässigkeit, wie die betrübliche Geschichte #PlaneBae zeigt¹¹⁸) ausgelöst werden, mit Beleidigungen und Bedrohungen, die nicht nur die Nutzung eines sozialen Netzwerks verunmöglichen, sondern sich auf das reale Leben auswirken, wenn Adresse, Namen der Partner und der Kinder sowie weitere persönliche Informationen mit dem Ziel der Schädigung verbreitet werden¹¹⁹. Die Hunderte oder auch Tausende, die solche Angriffe lancieren, inspirieren bzw. verlinken, können fast sicher mit Straffreiheit rechnen, da es praktisch unmöglich ist, sie zu identifizieren und zu verfolgen. Diese Gewissheit, sich nicht sorgen zu müssen, verleitet viele der Autoren dazu, mit offenem Visier zu handeln, was nebenbei gesagt auch die häufig geäusserte Ansicht widerlegt, dass «sich die Leute im Internet gehen lassen, weil sie anonym bleiben können»...

Zusätzlich zu den persönlichen Gesundheits- und Sicherheitsrisiken verursacht die zunehmende Digitalisierung der öffentlichen und privaten Infrastrukturen ein quasi-systemisches Risiko bei einem Blackout der Netzwerke, insbesondere bei den als kritisch eingestuften öffentlichen Infrastrukturen (Energie, Gesundheit, Kommunikation)¹²⁰.

«Data-Driven Policy»: Die Diktatur der Daten (und ihrer Experten)

Das Aufkommen der neuen Technologien, insbesondere von Big Data, erhöht das Gewicht von Daten als Beweisstücke in der öffentlichen Politik. Gewisse Leute träumen von einer post-aktuariellen bzw. post-versicherten Gesellschaft, in der das Risiko verschwinden muss, weil alles berechnet werden kann und vorhersehbar ist¹²¹. Andere glauben an das Ende des wissenschaftlichen Streits, weil alles bewiesen und gezeigt werden kann¹²². Nun ist aber nicht alles digitalisierbar (z. B. die Erschöpfung der Ressourcen, Träume, Utopien, Ideologien, Kunst, Kultur). Den aus Big Data hervorgehenden Daten wird eine «immanente Rationalität» zugesprochen; doch die Rationalität, auch wenn sie immanent ist, ist nicht die Wahrheit. Jedes Datenspiel verursacht zudem Fehler (und Umwege, vgl. oben S. 13 zur Diskriminierung); keines ist objektiv oder erschöpfend¹²³. Aufgrund von Daten entscheiden heisst angeblich objektiv entscheiden, doch das ist nicht Justiz, die fordert, dass man Tatsachen und Kontexte

berücksichtigt¹²⁴. Eine Entscheidung ist nicht deshalb richtig, weil sie der Berechnung folgt, sondern weil der, der sie trifft, sich rechtfertigen und an seinem Entscheid festhalten kann. Daneben sind unabhängig von der Qualität der genutzten Daten die Programmierungsfehler zahlreich: Im Schnitt gibt es auf 1000 Codierzeilen 50 Fehler. Und wenn der ursprüngliche Programmierer nicht mehr da ist, besteht ein hohes Risiko, dass niemand mehr etwas beherrscht¹²⁵. Gewisse auf KI spezialisierte Programmierer gehen im Übrigen so weit, dass sie Algorithmen «alchimistische» Lernfähigkeiten zutrauen¹²⁶. Das öffentliche Handeln auf Daten und Algorithmen zu gründen ist also kein Mittel für «gerechtere» öffentliche Entscheide (was auch immer der Begriff «gerecht» dann bedeutet).

Ein machtloser, nicht vertrauenswürdiger Staat?

Die digitale Revolution bringt aus Sicht der Sozialdemokraten, die sich schon immer für einen starken Staat sowie kollektive und demokratische Lösungen eingesetzt haben, ein grosses Risiko mit sich: den Verlust des Vertrauens in den Staat und dessen Fähigkeit zu schützen (vor Cyberrisiken, Massen-Cyberbelästigung, «sozialem Tod» usw.), souverän sein Recht zu bestimmen und anzuwenden, aber auch Dienstleistungen und Grundinfrastrukturen zu liefern, namentlich beim Zugang zu neuen Technologien und der entsprechenden Bildung. In der Stadt New York zum Beispiel gibt es so viele Airbnb-Inserate, die das Verbot, eine Wohnung mehr als 30 Tage zu vermieten, verletzen, dass es unmöglich ist, das Gesetz anzuwenden¹²⁷. Und angesichts des Aufstiegs der GAFAs zu einer Grossmacht ist die Fähigkeit der öffentlichen Behörden, den sozialen Zusammenhalt zu garantieren, beschränkt. Einige Förderer der neuen Technologien libertärer Gesinnung schliesslich wollen bestimmte, als «hoheitlich» betrachtete Vorrechte des Staates aufheben, z. B. die Kontrolle der Legalität von Immobilientransaktionen, die einem Blockchain-System anvertraut werden soll¹²⁸. Der Staat riskiert zudem, die (auch wirtschaftlichen) Grundfreiheiten nicht mehr schützen zu können (inklusive den Grundfreiheiten, die heute in der Bundesverfassung nicht als solche anerkannt sind, wie menschenwürdige Arbeit oder das Recht auf soziale Sicherheit); deren Inhalt droht auch in seiner Substanz ausgehöhlt oder von privaten Firmen diktiert zu werden. Die Teilnahme am digitalen Leben, also weitgehend am sozialen Leben an sich, verlangt immer stärker, dass man sich den von privaten Dienstleistungsanbietern festgelegten Regeln beugt, was häufig bedeutet, dass man die individuelle Freiheit aufgibt und via allgemeine Geschäftsbedingungen, die niemand in der Lage ist zurückzuweisen (und übrigens auch nicht zu lesen), auf einen grossen Teil der eigenen Grundrechte zu verzichten. Die Netzwerke können sich nicht mit einer grossen Menge einzelner Abkommen verstopfen; sie unternehmen deshalb alles, um ein generelles Einverständnis zu erlangen, so dass sie tun können, was sie wollen (wenn nötig über den Umweg von «Nudges»), unabhängig von den Gesetzesgrundlagen. Das «Ja, ich stimme zu» erfolgt eigentlich im Moment der ersten Auswahl (wenn es sich überhaupt um eine echte Auswahl handelt, vgl. weiter oben S. 15): «Will ich ein digitales Leben oder nicht?»¹²⁹. Danach kann man in der Regel keine Zustimmung mehr geben, vor allem wegen des «Lock-in-Effekts»: Da ein Recht auf Datenübertragbarkeit fehlt, wechselt man den Leistungsanbieter nicht mehr, wenn einmal alle Daten bei ihm sind, und alle Dienste, die man im Alltag braucht, miteinander verknüpft sind (sowie die einen ohne die anderen unbrauchbar werden)! Die Vereinbarung kann auch erpresst und die Selbstbestimmung auf null reduziert werden: So ist jemand, der sich weigert seine Daten für eine Statistik zu liefern, letztlich Teil dieser Statistik¹³⁰.

Wird die Menschheit zweitrangig?



Eine Risikoanalyse der digitalen Revolution muss, zumindest kurz, auch das «philosophische Risiko» der «technologischen Singularität» beleuchten, das heisst den Moment, in dem KI die menschliche Intelligenz übertrumpfen wird. Zum Beispiel sagte 2004 Larry Page voraus: «Google wird ins Gehirn der Leute eingebaut sein. Sie werden ein Implantat haben, und wenn sie an etwas denken, wird ihnen Google automatisch die Antwort liefern.»¹³¹. Manche sind der Meinung, die GAFA werden von einer Ideologie der Vorherrschaft der Technologie über den Menschen angetrieben¹³².

Die Furcht um die Singularität ist unseres Erachtens unbegründet. Natürlich schlägt KI den Menschen im Schach seit den 1980er Jahren... sie ist aber noch nicht fähig, die Figuren im Spiel korrekt zu bewegen, was wiederum menschliche Kinder schon in jungen Jahren können!

Wie auch immer, die Welt ist weder völlig modellierbar noch berechenbar. Wie Ito sehr richtig sagt, macht uns die Entwicklung von Rechnungsmacht nicht intelligenter, sondern nur fähig, besser zu rechnen. Es drängt sich deshalb auf, die KI nicht so sehr als Konkurrenz oder Ersatz zu sehen, sondern vielmehr als Ergänzung zur menschlichen Intelligenz¹³³.

(Le Chat, © Ph. Geluck, 1986)

Und schliesslich, wie auch immer die technologischen Fortschritte aussehen werden, gewisse menschliche Fähigkeiten werden vermutlich niemals auf Maschinen oder KI übertragbar sein, das diese z. B. Ungeschicklichkeit, Unvorhersehbarkeit, Instinkt, Intuition, Bionik¹³⁴, Empathie oder Emotionen nicht reproduzieren können.

5. Vorschläge: die Grundrechte an die digitale Revolution anpassen

Einführung

Seit jeher setzen sich die Sozialdemokraten für die Grundrechte ein. Sie waren immer auf der Seite der Nutzniesser der Grundfreiheiten und standen stets zuvorderst dafür ein, dass diese universell angewendet werden, aber auch dafür, überall dort neue Grundrechte zu schaffen, wo es nötig war. Die digitale Revolution bringt grosse Chancen, aber auch grosse Risiken für die Bevölkerung mit sich. Eine Stärkung der Grundrechte hilft dem Individuum, die Chancen zu nützen und sich gleichzeitig gegen die Risiken zu schützen. Jeder und jede hat das Recht, die Chancen der digitalen Revolution zu nutzen, wenn sie ihm oder ihr sinnvoll erscheinen; gleichzeitig wissen alle um ihren Schutz, wenn die Nutzung Risiken birgt.

Wir haben uns entschieden, einige der wichtigsten Grundrechte anzuschauen, die in der Bundesverfassung verankert sind. Unser Ansatz ist nicht juristisch, sondern politisch: Wir berücksichtigen also die Grundrechte, die einen Rechtsanspruch begründen, aber auch die Ziele, die sich der Bund gibt (Art. 2 BV), und die sozialen Ziele (Art. 41), die nicht justiziabel sind. Wir wollen nicht zwingend diese Rechte ergänzen oder neue schaffen, sondern prüfen,

wo ihre Auslegung oder ihre Umsetzung ins Gesetz präzisiert werden müssen. Wir haben auch einige zentrale Aufgaben des Staates untersucht, die, ohne eigentliche Grundrechte zu sein, besonders von der digitalen Revolution betroffen sind, wie z.B. die Definition der Identität oder der Service public.

Eine Charta oder eine neue Präambel für die Bundesverfassung?

Verschiedene Staaten denken darüber nach, wie sie die neuen, durch die digitale Revolution nötig gewordenen Grundrechte in der Verfassung verankern wollen. In Deutschland hat Minister Heiko Maas (SPD), einen Vorschlag von Martin Schulz (damals Kanzlerkandidat) aufnehmend, das Projekt einer «Internet-Charta: unsere digitalen Grundrechte» entworfen. In Frankreich schlagen die Mitglieder der parlamentarischen Arbeitsgruppe Fortezza/Frassa vor, die Verfassung mit einer Charta in der Präambel zu ergänzen. Diese würde keine neuen Rechte im engeren Sinn schaffen, sondern strebt an, einige grosse Prinzipien zu verankern, indem sie in diesem übergeordneten Text festgehalten werden. Die auf verschiedenen Ebenen garantierten Rechte und Freiheiten könnten so auf Verfassungsmässigkeit geprüft werden¹³⁵. Die beiden Projekte für eine Charta enthalten insbesondere folgende Rechte:

- Recht auf gleichberechtigten und nicht-diskriminierten Zugang
- Netzneutralität
- Ausbau der Netze im allgemeinen Interesse
- Die Digitalisierung erleichtert die Teilnahme am öffentlichen Leben und die öffentliche Debatte
- Recht auf Zugang zu Informationen, die für eine Debatte im öffentlichen Interesse nützlich sind
- Schutz persönlicher Daten und Selbstbestimmung in Sachen Information
- Recht auf Bildung und Weiterbildung im Bereich Digitalisierung
- Recht, sich gegen Algorithmen zu wehren
- Recht auf menschenwürdige Arbeit, auch online
- Gleiche Rechte online wie in der realen Welt
- Recht auf ein Leben «offline», in der «analogen» Welt
- Verbot des Missbrauchs durch Monopole und beherrschende Stellungen
- Auftrag an die Staaten, ein internationales Internet-Recht zu schaffen

Das französische Konzept einer Verfassungscharta ist allerdings (wie die Umweltschutzcharta von 2004) dem schweizerischen Verfassungsrecht fremd, das keine verfassungsrechtliche Gerichtsbarkeit kennt wie Frankreich oder Deutschland. Dennoch sind diese Projekte sehr nützlich, um zu bestimmen, welche Ergänzungen in unseren Katalog der Grundrechte aufzunehmen sind.

Art. 2 BV Zweck der Eidgenossenschaft

1 Die Schweizerische Eidgenossenschaft schützt die Freiheit und die Rechte des Volkes und wahrt die Unabhängigkeit und die Sicherheit des Landes.

2 Sie fördert die gemeinsame Wohlfahrt, die nachhaltige Entwicklung, den inneren Zusammenhalt und die kulturelle Vielfalt des Landes.

3 Sie sorgt für eine möglichst grosse Chancengleichheit unter den Bürgerinnen und Bürgern.

4 Sie setzt sich ein für die dauerhafte Erhaltung der natürlichen Lebensgrundlagen und für eine friedliche und gerechte internationale Ordnung.

Art. 2 BV braucht wegen der digitalen Revolution nicht ergänzt oder verändert zu werden; diese muss aber zu neuen Auslegungen führen, um die Risiken zu berücksichtigen, die sie mit sich bringt.

Die Schweiz muss also keine «digitale Kolonie» werden oder bleiben¹³⁶. Unser Land soll seine Souveränität im Internet stärken, indem es folgendes Prinzip anwendet: Jede Online-Aktivität, die Resultate oder Folgen in der Schweiz hat, ist schweizerischem Recht unterstellt, egal wo sich der Urheber, das Unternehmen, das die Dienstleistung(en) erbringt (auch wenn es eine Plattform ist, die eine Beziehung zwischen Lieferant und Kunde herstellt), seine Server, die Daten usw. befinden.

Die Schweiz muss weiterhin ihr eigenes Recht schaffen (oder dazu beitragen, dass internationales Recht entsteht, das sie anwenden wird) und sich nicht dem «Recht» unterstellen, das Private oder andere Staaten schaffen. Sie soll auch die Erarbeitung von neuen «digitalen Genfer Konventionen» anregen und daran mitarbeiten, um im internationalen Recht Regeln des Funktionierens der Netze und für deren Zugang sowie die durch die digitale Revolution nötig gewordenen neuen Grundrechte zu verankern; sie muss aber auch die Nichtverbreitung autonomer Waffen garantieren¹³⁷.

Ausserdem muss die Schweiz dafür sorgen, dass ihre kritischen Infrastrukturen geschützt sind, indem sie bei Problemen oder Hackerangriffen abgeschaltet werden (bzw. offline funktionieren) können.

Weiter muss die Schweiz dafür sorgen (aber diese Feststellung gilt unabhängig von der digitalen Revolution), dass der soziale Zusammenhalt garantiert wird, denn dieser ist gefährdet durch das Aufkommen von riesigen Unternehmen, die auf ihren eigenen Märkten über Monopole, aber auch die Möglichkeit verfügen, in irgendeinen anderen Markt einzutreten (auch mit Leistungen im Bereich des Service public), indem sie von Anfang an eine beherrschende Stellung erwerben. Die Akkumulation von Kapital durch die GAFSA setzt den sozialen Zusammenhang und den *allgemeinen* Wohlstand aufs Spiel, vor allem wenn sie sich der Steuerpflicht und dem Recht entziehen¹³⁸. Der soziale Zusammenhalt könnte aber auch durch das Ende der Solidarität bedroht sein, wenn der intensive Einsatz von Big Data den Unternehmen und öffentlichen Körperschaften, vor allem den Versicherungen, erlaubt, ihre «Jagd auf schlechte Risiken» zu optimieren, indem sie die Leistungen und ihre Finanzierung extrem individualisieren¹³⁹.

Art. 5 BV Rechtsstaat (siehe auch Verfahrensrechte in Art. 29, 29a, 30 und 32)

Ein Rechtsstaat muss von jeder Technologie, vor allem von Algorithmen, verlangen, dass sie seine Gesetze und sozialen Normen einhält¹⁴⁰. Unserer Ansicht nach ist deshalb Art. 5 zu präzisieren. Insbesondere muss die Anwendung folgender Grundsätze garantiert sein¹⁴¹:

- **Erklärbarkeit und Transparenz von KI und Algorithmen:** Das Funktionieren eines Algorithmus und die Daten, derer er sich bedient, müssen öffentlich gemacht und den betroffenen Personen gegenüber erklärt werden können (im Idealfall ohne dass man über besondere Kenntnisse in Informatik verfügen muss), erst recht, wenn es um eine staatliche Entscheidung geht (oder schlimmer noch: der Algorithmus die Entscheidung allein trifft). Von KI in «Blackboxes» getroffene Entscheidungen müssen protokolliert werden, damit man feststellen kann, wer für Fehler verantwortlich ist¹⁴². Allerdings läuft die Forderung nach Erklärbarkeit und Transparenz Gefahr, einem gewöhnlich Sterblichen nicht viel zu nützen, wie das Beispiel von «Parcoursup» zeigt, wo vom Ministerium 40 Dateien offen gelegt und dazu eine 20-seitige technische Dokumentation mit der detaillierten Auflistung der angewandten Techniken mitgeliefert wurden¹⁴³. Im Übrigen bleibt ein Algorithmus, erst recht, wenn er selbstlernend ist, eine schwierige, wenn nicht gar unverständliche «Blackbox» für die

Bevölkerung, die ja schon lange nicht mehr versteht, wie die meisten Maschinen im Alltag funktionieren, auch wenn sie lebenswichtig sind. Manche schliessen daraus, dass die Transparenz von Algorithmen eine Augenwischerei ist¹⁴⁴.

- **Verantwortlichkeit:** Bei jedem algorithmischen System muss es eine Person geben, die für unerwünschte Auswirkungen geradesteht.
- **Genauigkeit:** Fehlerquellen müssen identifiziert, protokolliert und verglichen werden.
- **Überprüfbarkeit:** Algorithmen müssen so entwickelt werden, dass sie von Dritten untersucht und in ihrer Wirkung korrigiert werden können. Die Ergebnisse und Kriterien dieser Evaluationen müssen erklärt und veröffentlicht werden.
- **Justiziabilität:** Um die Verzerrung von automatisierten Entscheiden zu vermeiden, müssen Algorithmen, die Entscheide über Individuen treffen, untersucht werden können, damit insbesondere ihre diskriminierende Wirkung messbar ist.

Art. 6 BV Individuelle Verantwortung

Art. 6 BV ist zu ergänzen, damit das für die Freiheit unerlässliche Pendant, die Verantwortung, besser geschützt ist. Die digitale Revolution schafft eine grosse Zahl an Situationen, die Schäden verursachen, für welche niemand verantwortlich ist bzw. die Verantwortlichen straffrei ausgehen, sei es, weil die Anzahl zu hoch oder die Identifikation schwierig ist, oder wegen Fragen der Extraterritorialität. Unserer Meinung nach gibt es jedoch nicht nur ein Grundrecht auf Beseitigung eines Schadens durch den Urheber (siehe weiter oben), sondern auch darauf, dass dieser Urheber eines Verbrechens oder Delikts strafrechtlich verfolgt wird (siehe weiter unten zu Art. 10 BV). Dazu braucht es aber eine verantwortliche natürliche oder juristische Person, ausser in den Fällen, die sich menschlicher Verantwortung entziehen (namentlich unvermeidliche Naturkatastrophen). Es darf also keine Schäden geben ohne Verantwortliche (Person oder Unternehmen), und auch keine Unternehmen ohne «menschliche» Verantwortung oder solche, deren Verantwortliche nicht kontaktiert werden können (weil sie z.B. nur via ein Online-Formular kontaktierbar sind, wo man nicht weiss, ob es von einem Chatbot behandelt wird oder überhaupt nicht). Das darf allerdings nicht dazu führen – denn das wäre absurd – dass gewisse autonome Maschinen ständig unter der Überwachung einer Person stehen (das Wiener Übereinkommen schreibt z.B. vor, dass jedes Fahrzeug einen «eingriffsbereiten» Fahrer haben muss, was dem Konzept der Autonomie widerspricht!). Im Moment akzeptieren einige Hersteller freiwillig die Übernahme der Verantwortung im Fall von Schäden durch ihr autonomes Produkt (Volvo, Google oder Mercedes)¹⁴⁵, aber sie bleibt ein freiwilliger Schritt.

Wie Art. 27 ZGB vorschreibt, gilt die individuelle Freiheit auch im Fall einer freiwilligen (und mehr oder weniger bewussten) Abtretung derselben, z.B. wenn man einen Grossteil seines Privatlebens aus Bequemlichkeit so verbringt, dass man die Verwaltung seines Haushalts einer Assistentin wie Alexa (Amazon) überlässt. Der Schutz der individuellen Freiheit muss auch verbessert werden, um die «Lock-in»- bzw. «Take it or leave it»-Effekte zu verhindern, die zur Folge haben, dass man, um einen Online-Service zu nutzen, die gesamten allgemeinen Bedingungen akzeptieren muss, ohne Möglichkeiten zur Verhandlung oder Alternativen zu haben, wenn der Erbringer, was häufig der Fall ist, ein Monopol besitzt. Schliesslich: Von individueller Verantwortung zu reden ist nicht logisch, wenn mangels Mittel zur Verringerung der digitalen Kluft (vgl. oben) nicht alle Zugang haben zu den Leistungen und Innovationen, welche die digitale Revolution anbietet.

Art. 7 BV Menschenwürde

Wir wollen nicht die Angst vor einem «Krieg gegen die Maschinen» oder vor der Singularität schüren, doch auf der Ebene der Menschenwürde könnten die Folgen der digitalen Revolution am stärksten sein. Die Mehrheit dieser Fragen verdient eine vertiefte ethische Diskussion, zu der beizutragen nicht unser Anspruch ist. Allerdings muss als Ergebnis dieser Debatte der Schutz der Menschenwürde auf jeden Fall durch die Verfassung präzisiert werden. Wir denken da insbesondere an folgende Themen:

Augmented Humanity

Die digitale Revolution ist geeignet, den Traum des Cyborgs, also des vernetzten, «erweiterten» Menschen zu realisieren. Der technologische Fortschritt ist so rasant, dass die Einpflanzung von Chips¹⁴⁶ und von intelligenten Prothesen keine Science-Fiction mehr ist. Die wichtigste Frage wird jene nach dem Recht am Nutzen von Innovationen sein: Werden sie z.B. zum Leistungskatalog von Sozialversicherungen gehören? Oder muss man sie stattdessen verbieten, um zu verhindern, dass die Ungleichheiten werden zunehmen? Oder eher aus ethischen Gründen?

Dann kommt die Frage der Pflicht. Wird es bei bestimmten Berufen oder Aktivitäten obligatorisch, eine Prothese zu tragen, die gewisse Aufgaben erleichtert oder erst möglich macht, oder ein Chip zur Lokalisierung bzw. der wesentliche Informationen speichert, vor allem für die Sicherheit ihrer Träger oder von Dritten? Wird es Eltern möglich sein, ihren Kindern oder Dritten, denen sie sie anvertrauen, solche Chips aufzuzwingen? Soll der Staat Personen, die er überwachen darf (Häftlinge) oder denen er gefährliche, komplexe (Chirurg, Techniker für Nuklearsicherheit) bzw. mühsame Arbeiten (Exoskelette für Bauarbeiter) anvertraut, dazu verpflichtet? Oder wenn er Statistiken braucht, z. B. zur Volksgesundheit¹⁴⁷?

Welche Interaktion von Menschen mit «intelligenten» Maschinen?

Der Fortschritt neuer Technologien führt dazu, dass wir es in vielen Situationen des täglichen Lebens nicht mehr mit einem menschlichen Gegenüber zu tun haben, sondern mit KI oder einem Roboter. Eine zu diskutierende Frage wird sein, ob es ein Recht geben soll, **sich KI, die sich als Mensch ausgibt, zu verweigern, oder zumindest zu wissen, mit wem man es zu tun hat**¹⁴⁸. Man wird auch ein Recht diskutieren müssen, **sich gegen Pflegeroboter zu wehren**, die von «Natur» aus ja gar keine menschliche, für die Pflege unerlässliche Qualitäten aufweisen (Empathie, Kreativität, soziale Beziehungen), die aber wegen dem Mangel an qualifiziertem Personal und der steigenden Lebenserwartung eine immer wichtigere Rolle in der Pflege und Betreuungsarbeit einzunehmen drohen¹⁴⁹. In Japan stört sich bereits niemand mehr daran, von einem Roboter gestreichelt zu werden (eine inzwischen übliche Situation), denn die Leute haben sich schon lange an ein Leben mit Robotern gewöhnt, und ausserdem vermittelt der Shintoismus ein positives Bild von Maschinen¹⁵⁰.

Auf jeden Fall ist es unabdingbar, **für die Konzeption, Fabrikation und Nutzung von Robotern und KI einen ethischen Rahmen zu setzen**, so wie die Vorschläge, die in der EU auf dem Tisch liegen¹⁵¹.

Menschen im Dienst von Robotern/KI?

Immer öfter werden sich Menschen Algorithmen anpassen müssen. Das kann in nicht-expliziter Art geschehen, zum Beispiel wenn KI die Menschen zwingt, sich in einer Art und Weise zu verhalten, von der sie denken, dass die KI sie als positiv oder akzeptabel beurteilt (siehe S. 12 zu den Programmen, die «verdächtiges Verhalten» an Flughäfen erkennen). Oder in expliziter Weise, wenn z. B. ein Roboter ermächtigt ist, Arbeitern, mit denen er «zusammenarbeitet», Weisungen zu erteilen, (das ist beim japanischen Hitachi oder bei

Amazon bereits der Fall, deren Algorithmen praktisch jeden Schritt im Arbeitsprozess diktieren¹⁵²), oder wenn es ein Algorithmus ist, der entscheidet, ob Personal angestellt oder entlassen wird¹⁵³. Gewiss, weder ein Roboter noch KI sind juristische Personen, die in der Lage sind, Entscheidungen mit juristischen Folgen zu treffen, aber es wird öfter vorkommen, dass Arbeitgeber ihr Personal anweisen, diesen «Direktiven» Folge zu leisten, bzw. blind der «Empfehlung» folgen, Leute einzustellen oder zu entlassen, die der Algorithmus getroffen hat. Das würde darauf hinauslaufen, Menschen in den Dienst von Maschinen zu stellen, die Entscheide treffen könnten, welche nicht nur punktuell und auf einen Arbeitsprozess beschränkt sind, sondern grosse Folgen für das Leben der betroffenen Person haben können. Wie auch immer, es ist nötig, Art. 7 BV zu ergänzen, um ein neues Grundrecht, ausgehend von der Menschenwürde, zu schaffen, damit **kein menschliches Wesen Objekt oder Subjekt eines Algorithmus wird¹⁵⁴ und jede wichtige Entscheidung¹⁵⁵ einzig und allein von Menschen getroffen werden darf¹⁵⁶, bzw. die Menschen das Recht bekommen, jede Entscheidung, die von einem Algorithmus oder mit dessen Hilfe getroffen wird, abzulehnen, wenn diese der Menschenwürde widerspricht**. Ausserdem muss bei einer von KI oder mit ihrer Hilfe getroffenen Entscheidung eine (natürliche oder juristische) Person die Verantwortung übernehmen.

Was bleibt von den rein menschlichen Qualitäten und Mängeln?

Das Recht auf Menschenwürde bringt auch jenes mit sich, rein menschliche Mängel zu akzeptieren oder Qualitäten zu haben, wie das Recht, unvorhersehbar zu sein¹⁵⁷, Pläne und Meinungen zu ändern, nach Instinkt oder nach Gefühl zu handeln. Wenn es auf den Versuch hinausläuft, alles zu formen, zu messen, vorauszusehen und zu berechnen, dann ist die Anwendung neuer Technologien sicher nicht mit dem Begriff der Menschenwürde vereinbar.

Neues Grundrecht auf menschenwürdige Arbeit (nicht nur online)

Weil in unserem Leben die Arbeit so wichtig ist, muss aus der Menschenwürde ein Recht auf menschenwürdige Arbeit abgeleitet werden. Es ist weiter unten (S. 35) beschrieben.

Art. 8 BV Rechtsgleichheit

Es ist zwingend dafür zu sorgen, dass das Prinzip der Rechtsgleichheit auch auf automatisierte Entscheide angewendet wird, die ein erhöhtes Risiko für Diskriminierung (vgl. oben S. 13) darstellen. Dafür sind die Grundsätze gemäss Art 5. BV anzuwenden, ergänzt durch eine **Umkehr der Beweislast: Wer immer einen automatischen Entscheidungsprozess einsetzt, muss beweisen, dass dieser nicht diskriminierend ist¹⁵⁸**. Es könnte nämlich Opfern von Diskriminierung unmöglich sein zu beweisen, dass sie Opfer geworden sind, denn dafür müsste man ja vor allem wissen, auf welche Daten sich die Entscheidung stützt, welche Qualitäten und allfällige Verzerrungen sie enthält.

Art. 9 BV Willkürverbot

Das Willkürverbot, eines der zentralen Elemente unseres Rechtsstaats, muss präzisiert werden, damit garantiert ist, dass es auch auf automatisierte Entscheidungen angewendet wird, vor allem, dass diese den Kontext und die individuellen Situationen einbeziehen, die nicht unbedingt als Modell darstellbar oder in Daten übersetzbar sind. Siehe auch die oben ausgeführten Prinzipien.

Es ist zu betonen, dass die Frage der automatisierten Entscheidungen nicht allein aus dem Blickwinkel des Datenschutzes (vgl. Art. 15 E-DSG) behandelt werden kann, wie das leider

heute der Fall ist, schon nur weil die Gesetzgebung zum Datenschutz nur Daten mit persönlichem Charakter behandelt (vgl. weiter unten S. 30 zum Kollektivrecht der Daten).

Art. 10 BV Recht auf Leben und auf persönliche Freiheit

Art. 10 BV ist zu ergänzen, damit er das Recht auf Leben und auf persönliche Freiheit trotz der digitalen Revolution besser garantiert.

Massnahmen zum Schutz des Rechts auf «physisches» Leben

Die digitale Revolution birgt neue Risiken für die physische Integrität und Gesundheit: von Robotern (nicht nur «Tötungsrobotern») und anderen autonomen Geräten verursachte Gefahren, Folgen für die körperliche und geistige Gesundheit wegen der ständigen Hyperkonnektivität, neue Umweltrisiken. Das Recht auf Leben ist genügend klar und braucht auf Verfassungsebene nicht ergänzt zu werden, seine Anwendung muss jedoch auf Gesetzebene präzisiert werden.

Insbesondere müssen Massnahmen gegen die Straffreiheit getroffen werden, welche die digitale Revolution aus obgenannten Gründen fördert. Das Recht auf Leben (Art. 10 BV und Art. 2 EMRK) schliesst nämlich das Recht eines Opfers auf Strafverfolgung ein, auch gegen häusliche Gewalt, aber auch eine Pflicht zum Schutz gegen gefährliche Technologien¹⁵⁹. Im Übrigen muss das Recht auf körperliche und geistige Unversehrtheit präzisiert werden mit Massnahmen gegen die Hyperkonnektivität, die ständige Erreichbarkeit und die dauernde Überwachung, nicht nur am Arbeitsplatz.

Massnahmen gegen den «sozialen Tod»

Das Recht auf Leben muss ergänzt werden durch ein Recht, das gegen den sozialen Tod schützt (vgl. oben S. 18), welcher ein Schritt auf dem Weg zum «realen» Tod (als Folge von Gewalt oder als Suizid) sein kann. Zu denken ist namentlich an Massen-Cybermobbing durch einen «digitalen Überfall» mit dem Ziel, dem Opfer zu schaden¹⁶⁰, entweder durch die Veröffentlichung des Privatlebens von jemanden ohne dessen Einwilligung¹⁶¹, oder durch eine Privatisierung der Justiz (und einer totalen Unterdrückung der Verfahrensrechte wie der Unschuldsvermutung oder dem Recht auf Anhörung), wenn eine schuldige Person oder ein mutmasslich Schuldiger der Anprangerung in den sozialen Medien und den Mitteln der Massenkommunikation (z. B. mit: #balancetonporc) ausgesetzt wird. Zu den Massnahmen gehört insbesondere die Etablierung einer **Gesamtverantwortung des sozialen Netzwerks, das keine Massnahmen ergreift, um solche Phänomene zu identifizieren oder zu stoppen bzw. solche Handlungen gar toleriert**. Dies erst recht, wenn es unmöglich ist, die Urheber zu identifizieren und ihrer habhaft zu werden, weil sie zu viele sind. Man muss auch **Straftaten wie Mobbing, Drohung oder Nötigung präzisieren**, damit die Teilnahme an einem digitalen Angriff, selbst wenn es sich als Einzelhandlung nicht um eine strafbare Tat handelt, vom Moment an strafbar wird, wo klar wird, dass es eine Massenaktion ist.¹⁶²

(Wieder)herstellung der individuellen Freiheit in der digitalen Welt

Wie oben erläutert, tendiert die digitale Revolution dazu, die individuelle Freiheit massiv einzuschränken, sei es, indem sie die Nutzer von digitalen Leistungen gleichsam zu Gefangenen (eines Anbieters mit Monopol oder einer Palette von miteinander verlinkten Diensten) macht oder ihnen jede Wahlfreiheit und Verhandlungsmöglichkeit nimmt, sobald sie eine alternativlose Vertragsbindung eingehen. Dies geschieht vor allem durch die (andernorts beschriebenen) Massnahmen, um die Macht der GAFA einzuschränken, aber auch durch eine Stärkung des digitalen Service public und die Entwicklung neuer Rechte für die

Nutzer, insbesondere bei der Datenübertragbarkeit, Recht auf Online-Anonymität, Stärkung der Regel für Einverständniserklärung oder Anfechtung von allgemeinen Geschäftsbedingungen.

Neues Grundrecht, die neuen Technologien nicht nutzen zu müssen

Die Online-Freiheit umfasst auch die Freiheit ...nicht online sein zu müssen, nicht vernetzt zu sein und keine online-Dienstleistungen zu nutzen. Egal aus welchen Gründen: keine oder eine zu geringe Kenntnis über das Funktionieren der Netze und der Dienstleistungen, kein Zugang zu den Technologien (warum auch immer), keine Lust, sich den Bedingungen der Dienstleister zu unterwerfen, keine Lust darauf, dass das Verhalten verfolgt, analysiert, zerlegt wird, das Recht, seine Daten zu schützen und anonym zu bleiben usw. **Der Begriff der persönlichen Freiheit muss deshalb so ergänzt werden, dass jedermann das Recht auf eine analoge Welt hat**¹⁶³. Dieses Recht muss insbesondere einschliessen, dass alle öffentlichen Leistungen (und jene der Service-public-Unternehmen) bezogen werden können, ohne dazu ein besonderes Kommunikationsmittel zu benötigen¹⁶⁴.

Art. 11 BV Schutz von Kindern und Jugendlichen

Der Kinderschutz ist sicher eines der Grundrechte, das verdient, im Zusammenhang mit der digitalen Revolution ergänzt und präzisiert zu werden. In vielen Fällen wird es darum gehen, die Kinder vor ihren Eltern (oder deren Vernachlässigung) zu schützen, die – in der Regel aus Bequemlichkeit oder unbewusst – das virtuelle und das reale Leben der Kinder den GAFA (sowie anderen öffentlichen oder privaten Körperschaften) ausliefern. Die digitale Revolution treibt viele Familien dazu, persönliche Daten ihrer Kinder via vernetzte Dinge weiterzugeben (nicht nur zu ihrer Überwachung), wie die vernetzten Plüschtiere CloudPets zeigen, die leicht zu hacken sind, oder der vernetzte Schnuller Pacifi-i. Die Kinder sind auch der Macht der digitalen Riesen ausgesetzt, wenn der ganze Haushalt unter die Kontrolle und Überwachung von Assistenten wie Alexa (Amazon) oder Home (Google) kommt.

Art. 11 müsste deshalb so ergänzt werden, dass die digitale Integrität der Kinder und Jugendlichen speziell geschützt ist, insbesondere um zu vermeiden, dass Dritte sich nicht nur der persönlichen Daten bemächtigen, sondern vor allem auch der Kontrolle über einen Teil ihres «realen» Lebens (selbst als Folge von elterlicher Vernachlässigung), solange sie nicht selber in der Lage sind, ihre Grundrechte geltend zu machen (siehe Art. 11 Abs. 2 «Sie üben ihre Rechte im Rahmen ihrer Urteilsfähigkeit aus»). Es müsste ein echtes Grundrecht des Sozialziels gemäss Art. 41 sein, das postuliert, dass «Kinder und Jugendliche in ihrer Entwicklung zu selbstständigen und sozial verantwortlichen Personen gefördert und in ihrer sozialen, kulturellen und politischen Integration unterstützt werden».

Die Rechte von Kindern und Jugendlichen sind zudem durch ein **neues Verfassungsrecht auf digitale Bildung** (nicht nur für Kinder) zu ergänzen, das weiter unten erläutert wird. Schliesslich müssen die geltenden Regeln zum Kinderschutz vor allem in Sachen Verbot und Begrenzung von Kinderarbeit strikter angewendet werden, insbesondere für junge Youtuber, die sich auf Anregung ihrer Eltern selber inszenieren oder gegen ihren Willen in Videos mit kommerziellem Ziel eingesetzt werden, wenn sie nicht gar belästigt oder gedemütigt werden, um ein Publikum zu generieren¹⁶⁵. Man müsste auch eine Anwendung dieser Regeln ins Auge fassen, um zu verhindern, dass Kinder, auch kleine, geisttötenden Videos und/oder Werbefilmen ausgesetzt werden¹⁶⁶.

Art. 12 BV Recht auf Hilfe in Notlagen

Der Zugang zu den digitalen Basisnetzwerken und -diensten muss als Teil der Minimalbedingungen für eine menschenwürdige Existenz betrachtet werden. Wenn nötig ist Art. 12 BV zu ergänzen, ebenso die geltenden Normen der Sozialhilfe und der Ergänzungsleistungen.

Art. 13 BV Schutz der Privatsphäre

Der Datenschutz ist sicher das meistdiskutierte Thema der digitalen Revolution und Gegenstand vieler Vorschläge, von denen gegenwärtig einige im Rahmen der Revision des DSG (*Privacy by Design, by Default, Control by Design, Privacy Impact Assessment, Recht auf digitales Vergessen* usw.) in Diskussion sind. Wir werden deshalb nur auf einige weniger oft diskutierte Aspekte eingehen.

Übertragbarkeit statt Eigentum der Daten

Ein (Individual-)Recht auf Eigentum von persönlichen Daten einzuführen, ist keine gute Idee. Es gibt Leute, die eine Art «digitales Grundeinkommen» fordern, finanziert durch den Verkauf (an den Meistbietenden) der persönlichen Daten. Auch ohne so weit zu gehen: Die Idee, aus seinen Daten eine Art Tauschwährung zu machen, ist weit verbreitet und auch schon ausprobiert worden, vor allem von Personen in prekärer Lage, die gezwungen sind, ihr Privatleben aufzugeben, um ein wenig Geld zu verdienen, indem sie z.B. an Umfragen teilnehmen, die ein paar Franken einbringen. Aber: Eigentum an seinen Daten, und damit die Möglichkeit, sie zu verkaufen, ist nicht ohne Risiko. Zunächst besteht die Gefahr einer Bemächtigung aller Daten (einschliesslich der nicht-persönlichen) und also reiner Informationen¹⁶⁷. Dann gäbe ein Eigentum an den Daten all jenen eine grosse Macht, die im Besitz der Quelle sind, aber auch jenen mit der entsprechenden Speicherkapazität (Amazon ist Weltmarktleader der *Cloud*). Ausserdem kann die Grenze zwischen persönlichen und unpersönlichen Daten schwierig zu definieren sein, was für rechtliche Unsicherheit sorgen könnte. Schliesslich gleicht das Eigentum an Daten nicht zwingend das gegenwärtige Ungleichgewicht der Kräfte aus, das den vertraglichen Datenaustausch stört, und sei es nur wegen des Besitzverlusts, der die Folge jeglichen Verkaufs ist, während heute die persönlichen Daten, selbst nach einer Übermittlung, «geschützt» sind.

Angebracht ist deshalb die **Gewährleistung eines Recht auf Übertragbarkeit der persönlichen Daten**, sofern dem Individuum ein Recht auf Verhandlungsmacht zugestanden wird, wenn eine neue Vertragsbeziehung eingegangen wird; so wird verhindert, dass man, wenn man von einem neuen digitalen Dienst profitieren oder den Provider wechseln will, «mit den Daten kommen muss». Die Übertragbarkeit von Daten zu garantieren könnte die Bürger auch dazu bewegen, ihre Daten bei Vorhaben im öffentlichen Interesse zu teilen¹⁶⁸.

Ein Recht auf Datensicherheit

Es ist eine Sache, Daten unter Einhaltung der Grundrechte der betroffenen Personen zu behandeln, und eine andere, sie so zu speichern, dass sich Dritte ihrer nicht bemächtigen können und den bisher garantierten Schutz auf null senken. Kürzlich hat ein mit Amazon vernetzter Lautsprecher des Typs Echo ein privates Gespräch eines Paares ohne deren Wissen aufgenommen und irrtümlich an einen Angestellten des Ehemanns¹⁶⁹ geschickt. Die Folgen von Datendiebstahl oder -verlust sind umso bedeutender, als die Technologien an Bedeutung und Macht zunehmen. **Es muss deshalb ein Grundrecht auf eine sichere Verwahrung von Daten gewährleistet werden**¹⁷⁰, mit abschreckenden Sanktionen für jene, die nicht alles unternehmen, was man vernünftigerweise für die Garantie dieser Sicherheit verlangen kann.

Ein klares Verfassungsrecht auf informationelle Selbstbestimmung

Art. 13 BV ist schlecht formuliert, denn selbst wenn das Recht auf Selbstbestimmung von der juristischen Praxis bestätigt wurde, schützt eine wörtliche Auslegung¹⁷¹ nur die missbräuchliche und nicht die gewöhnliche Verwendung von persönlichen Daten. **Das Recht auf Privatsphäre muss deshalb ein eigentliches Recht auf informationelle Selbstbestimmung (oder digitale Integrität) sein, das heisst, das Recht eines jeden zu bestimmen, ob und zu welchem Zweck seine Daten verwendet werden dürfen**¹⁷².

Für ein klares Recht auf Anonymität, Kryptographie und Verschlüsselung

Wir verhalten uns nicht gleich, wenn wir uns anonym in einer Masse bewegen, wie wenn wir wissen, dass wir als Individuum identifizierbar sind. Anonymität ist also ein Mittel, die Freiheiten zu schützen. Die Erklärung des Europarats vom 28. Mai 2003 über die Freiheit der Kommunikation im Internet widmet der Anonymität ihren Grundsatz 7: «Um den Schutz vor Online-Überwachung zu garantieren und den freien Ausdruck von Informationen und Ideen zu fördern, müssen die Mitgliedstaaten den Wunsch der Internetnutzer, ihre Identität nicht preiszugeben, respektieren. Das darf die Mitgliedstaaten aber nicht daran hindern, Massnahmen zu treffen und unter sich zusammenzuarbeiten, um Urheber von Straftaten ausfindig zu machen, die sie gemäss der nationalen Gesetzgebung, der Konvention zum Schutze der Menschenrechte und Grundfreiheiten und anderer internationaler Verträge im Bereich Justiz und Polizei begangen haben.» Weiter in den erläuternden Fussnoten zur Erklärung: «[...] die User können einen guten Grund haben, weshalb sie ihre Identität nicht preisgeben wollen, wenn sie sich im Internet äussern. Ihnen eine Preisgabe aufzuzwingen könnte in massiver Weise ihre Meinungsäusserungsfreiheit beschneiden. Dies würde auch der Gesellschaft potenziell wichtige Ideen oder Informationen vorenthalten. [...] Die User müssen vor jeder von öffentlichen oder privaten Körperschaften nicht erlaubten Online-Überwachung geschützt sein.»

Das Recht auf Anonymität (aber auch: das Recht auf Verschlüsselung und Kryptographie, Verbot von Fallen, Förderung von Kryptographie und Verschlüsselung von A bis Z) ist zwar bereits im Recht auf Privatsphäre als abgeleitetes Recht enthalten, muss aber gestärkt werden, indem es explizit in die Verfassung aufgenommen wird¹⁷³.

Re-Identifikation verhindern

Ein Pendant zum Recht auf Anonymität ist die Verhinderung der **Re-Identifikation** dort, wo anonymisierte Daten verwendet werden¹⁷⁴. Man muss deshalb verlangen, dass bei jeder Datenverarbeitung eine **vorgängige Analyse** des Risikos einer Re-Identifikation erfolgt und, wenn nötig, **präventive Massnahmen ergriffen werden**, um eine solche zu verhindern. Im Übrigen darf die Verwendung von anonymisierten Daten (oder die Absicht dazu) nicht genügen, die Verantwortlichen der Verarbeitung von jeglicher Verantwortung zu entbinden.

Ein Recht auf freien Datenverkehr?

Die Verfechter des freien Marktes und Verhinderer von Einschränkungen desselben fordern immer deutlicher einen freien Datenverkehr nach dem Vorbild der 4 Grundfreiheiten der EU. Die Europäische Kommission arbeitet gegenwärtig Vorschläge in diese Richtung aus. Ein solcher Mechanismus, der zweifellos die GAFAs und andere grosse multinationale Firmen begünstigen würde, ist unserer Meinung nach abzulehnen, vor allem solange internationale Standards fehlen, die den Schutz der Daten in allen Ländern garantieren und verhindern, dass der Schutz vor den Nachteilen der digitalen Revolution untergraben wird. Wir schliessen uns

der vorsichtigen Haltung des CNNum an, der wie folgt Stellung nimmt: «Eine Einführung des Grundsatzes des freien Datenverkehrs zum gegenwärtigen Zeitpunkt könnte noch schlecht abzusehende Folgen nach sich ziehen angesichts der extrem unterschiedlichen Realitäten, die vom Begriff Daten abgedeckt werden und der Vielfalt der Anwendungen und Märkte, welche die Daten noch hervorbringen könnten. Es scheint zentral zu sein, sich eher Fragen zu stellen über die konkreten Aktionen, die unternommen werden müssen, um Europa zu ermöglichen, von den ökonomischen und sozialen Folgen der digitalen Revolution zu profitieren, statt sich einem neuen Prinzip zu unterziehen. Ausserdem ist der Rat der Meinung, dass die Hindernisse beim Datenverkehr weniger bei den nationalen Grenzen liegen als vielmehr auf der Ebene der Lock-in-Strategie und Vorratsdatenspeicherung zwischen Wirtschaftsakteuren. Es sind deshalb ebenso sehr die Hindernisse des Datenverkehrs zwischen den Plattformen wie zwischen den Grenzen, welche die Kommission aufheben müsste. Schliesslich könnte die Anerkennung eines Prinzips für den Datenverkehr auf europäischer Ebene ein Argument darstellen, den Grundsatz in zukünftige Abkommen zum freien Austausch aufzunehmen. Das würde den Datenverkehr ohne Kontrolle erleichtern (...).»

Ein kollektives Datenrecht

Der Datenschutz leidet gegenwärtig an einem schweren Fehler: er schützt nur «persönliche» Daten. Dabei erlauben viele Verwendungen von Daten ohne Verbindung zu Individuen, diese dennoch zu identifizieren, oder sie können diskriminierende Folgen für sie haben (vgl. oben S. 13 zu automatisierten Entscheiden und den Diskriminierungen, die sie verursachen können). Ein Beispiel dafür sind die unpersönlichen Daten, die von einem Telekomprovider gesammelt werden, wenn er einer Gemeinde hilft, eine «Smart City» zu werden. Um diesem «toten Winkel» etwas entgegenzusetzen, rät Villani zu Recht zur Schaffung eines **Kollektivrechts zum Datenschutz, damit es dem Individuum möglich ist, sich gegen die Folgen einer Verwendung von nicht-persönlichen Daten für seine persönliche Situation zu schützen**¹⁷⁵. Ausserdem muss die Möglichkeit für ein **Sammelklagerecht in Sachen Datenschutz** eingeführt werden, einerseits um den betroffenen Personen die Möglichkeit zu geben, sich als Gruppe gegen die Verwendung von Daten zu wehren, welche sie als Gruppe benachteiligt, aber andererseits auch wegen des geringen Streitwerts in Bezug auf persönliche Daten, der das «Preis-Leistungs-Verhältnis» eines rechtlichen Vorgehens unverhältnismässig macht, es sei denn, man verfüge über die Zeit, die Mittel und den Willen, die nötig sind, um eine Grundsatzentscheidung herbeizuführen, wie das zum Beispiel Max Schrems gegen FB gemacht hat.

Zudem: Wenn das Teilen von anonymisierten (und nicht re-identifizierbaren, siehe oben!) Daten (z.B. im Gesundheitswesen, beim Transport, bei den natürlichen Ressourcen, Energieverbrauch, Boden- und Gebäudenutzung usw.) im öffentlichen Interesse ist¹⁷⁶, muss **eine Pflicht (für Personen und Unternehmen) für das Teilen ihrer Daten** angestrebt werden. Die Lösung könnte mit dem Mechanismus vergleichbar sein, der beim geistigen Eigentum oder der Verwendung von «*Essential Facility*» spielt, das heisst dass der Besitzer einer unerlässlichen Infrastruktur, die zu duplizieren nicht sachdienlich wäre, diese zu einem vernünftigen Preis zur Verfügung stellt.

Allerdings darf das kollektive Datenrecht sich nicht damit begnügen, die User bei einem Missbrauch von kollektiven Daten zu schützen. Es ginge vielmehr darum, aus **Daten ein gemeinsames Gut zu machen**, ein öffentliches, auf demokratische Art verwaltetes Gut, wie es insbesondere Morozov vorschlägt¹⁷⁷. **Daten sind schon lange ein wesentliches Gut, eine Infrastruktur des Service public, die in Kollektivbesitz sein sollte**. Statt deren Besitz privaten Unternehmen zu überlassen, die dem Nutzer ein Zugriffsrecht auf Daten aufzwingen, die sie eigentlich selber produziert haben, wäre es besser, die Sache umzukehren und den

öffentlichen Institutionen die Entscheidung darüber zu überlassen, wer welche Daten, zu welchem Zweck und zu welchem Preis verwenden darf¹⁷⁸.

Art. 16 und 17 BV Meinungs-, Informations- und Medienfreiheit

Medienförderung und der Kampf gegen Falschinformationen (*Fake News*)¹⁷⁹ sind Themen, die schon breit diskutiert werden und Gegenstand zahlreicher Vorstösse vor allem von Seiten der SP sind.

Dennoch sind die Probleme zu betonen, die durch die Vorherrschaft bestimmter Webseiten wie Google oder durch die sozialen Medien bei der Verbreitung von Medieninhalten verursacht werden. Diese bedroht die Vielfalt: Die Schliessung von BuzzFeed France (am 7.6.18) hat gezeigt, dass die Änderung des Algorithmus bei FB (Bevorzugung von Veröffentlichungen von «Freunden» zulasten derjenigen von Medien, auch wenn sie seriös sind) einige «*Pure Players*» wie brut.fr in Schwierigkeiten gebracht hat, die seither weniger sichtbar sind und damit weniger geteilt werden, was ihr Geschäftsmodell in Gefahr bringt¹⁸⁰.

Art. 26 BV Recht auf Privateigentum

Selbst wenn das Recht auf Privateigentum nicht zu den von den Sozialdemokraten geliebten Grundrechten gehört, ändert das nichts daran, dass es durch das Aufkommen der vernetzten Dinge mehr und mehr beschnitten wird. Es ist nämlich schwierig, sich als Eigentümer eines vernetzten Dings zu sehen, dessen Grad der Vernetztheit man nicht nach eigenem Gutdünken lenken kann. Das Ding kann unbrauchbar oder gefährlich werden, wenn es gehackt wird¹⁸¹, oder, noch einfacher, wenn eine gute Netzverbindung fehlt, wie der kürzliche Fall eines Tesla zeigt, der nicht mehr geöffnet werden konnte, weil er auf dem Parkplatz, wo er abgestellt war, keine Verbindung hatte – was leicht schwere Folgen für das Baby hätte haben können, das sich im Auto befand¹⁸². Aber über die simple Frage der Netzverbindung hinaus sind die Besitzer eines vernetzten Gegenstands in der Regel abhängig vom Betriebssystem, dessen Optionen, dessen API, der Aktualisierung, der Kompatibilität mit der Hardware usw. **Es ist deshalb angezeigt, Art 26 BV so zu präzisieren, dass dieser in jedem Fall das Recht des Eigentümers einschliesst, zu kontrollieren, ob und wie das fragliche Objekt vernetzt ist (*Control by Design*).**

Privatrechtlich könnte sich auch bald die Frage nach der Garantie des Grundrechts durch den Staat stellen, nämlich wegen des Erfolgs der Blockchain, der zu einer Privatisierung dieser Garantie ausserhalb jeder öffentlichen Kontrolle und Legitimität führen könnte¹⁸³.

Art. 27, 94 und 96 BV Wirtschaftsfreiheit

Die digitale Revolution fördert eine wohlbekannt Tendez des Kapitalismus: sich auf die Regeln der freien Konkurrenz berufen, um sie dann besser zu unterdrücken, sobald man ein privates Monopol errichtet hat. Auch wenn die Konkurrenz und der freie Markt nicht in allen Bereichen erwünscht sind, ist dafür zu sorgen, dass sie dort funktionieren, wo sie es sind¹⁸⁴. Das Kartellrecht ist das Instrument des Staates, um zu verhindern, dass sich der Markt selber torpediert. In der Schweiz neigt das Gesetz dazu, die grossen Unternehmen zu bevorzugen, indem es das Kriterium der Effizienz privilegiert¹⁸⁵, was angesichts der Macht der GAFA besonders schädlich ist für die Wirtschaft. Ausserdem profitieren Letztere ohnehin vom Missbrauch einer beherrschenden Stellung: Man kann auch mit einem Marktanteil von 5% in mehreren Ländern weltweit eine beherrschende Stellung einnehmen¹⁸⁶. Allerdings zeigt die Rekordbusse für Alphabet (Google), die am 18. Juli 2018 durch die Europäische Kommission¹⁸⁷ ausgesprochen wurde, die Möglichkeiten des Eingreifens der Behörden auf der Basis des Wettbewerbsrechts auf, aber gleichzeitig auch die Mängel dieses Rechts: Selbst

wenn die Busse gigantisch erscheinen mag (über 4,3 Milliarden Euro), ist sie dennoch nur ein Klacks im Vergleich zu den rund 90 Milliarden USD an flüssigen Mitteln, über die Alphabet verfügt. Zudem brauchte es ein 7 Jahre dauerndes Verfahren, um Google zu verurteilen, das in der Zwischenzeit problemlos seine dominierende Stellung ausbauen konnte (85% Marktanteil bei den mobilen Apps). Dies erinnert an den Fall von vor 20 Jahren, bei dem der Internet Explorer (Microsoft) dem Browser Netscape gegenüberstand. Netscape wurde aus dem Markt gedrängt, in dem er Pionier war, und war bereits verschwunden, als die Verurteilung von Microsoft wegen missbräuchlicher Praktiken in Kraft trat.

Der Machtzuwachs der GAFa ist aber nicht nur schädlich für die Allgemeinheit, weil er das gute Funktionieren der Märkte gefährdet. Vor allem wegen der weiter oben beschriebenen Bedrohung, den diese Unternehmen für den Service public, die Glaubwürdigkeit des Staates und dessen Finanzierung, die Einhaltung der Grundrechte und den gesellschaftlichen Zusammenhang darstellen, darf ihre Existenz von den Demokratien nicht mehr geduldet werden. **Die GAFa sind zu einem systemischen Risiko geworden. Ihre Zerschlagung wäre wünschenswert, um nicht zu sagen notwendig. Art. 96 BV ist deshalb mit dem Ziel zu modifizieren, dass ihre Aktivitäten in der Schweiz aufgeteilt werden, indem man die Datenquellen / die Suchmaschine von den Diensten trennt, die diese Daten nutzen.**

Man darf sich jedoch nicht einfach auf frühere spektakuläre Zerschlagungen von monopolistischen Unternehmen wie Standard Oil oder AT&T abstützen, denn diese betrafen Unternehmen, deren Monopole sich auf ein klar umrissenes Staatsgebiet konzentrierten und deren Beziehung zum Staat, zu den Kunden, Lieferanten und Arbeitern von diesen territorialen Grenzen¹⁸⁸ geprägt war. Man darf sich auch nicht zufriedengeben mit Sanktionen – theoretisch nach Art. 49a KG in der Schweiz möglich – wie im Fall Google (siehe oben), nicht nur weil die Unternehmen genügend gross sind, um diese schmerzlos aus der Portokasse zu bezahlen, sondern vor allem weil sie ja nicht nur wegen der wettbewerbsschädigenden Praktiken gefährlich sind, sondern wegen ihrer Grösse und ihres Geschäftsmodells.

Art. 34 BV Politische Rechte

Die jüngsten Ereignisse machen eine **Präzisierung von Art. 34 für einen besseren Schutz des Meinungsbildungsprozesses sowie gegen die Beeinflussung von Abstimmungen online**¹⁸⁹ nötig. In diesem Zusammenhang scheint es gewagt, um nicht zu sagen unvernünftig, den demokratischen Prozess oder Teile davon zugunsten von Online-Tools zu verändern (*E-Voting*, *E-Collecting*, *Civic Software*, Smartvote- oder Vimentis-«Wahlprofile»). Im Übrigen ist zwar das Aufkommen neuer Tools zu begrüßen, wenn es die Beteiligung und Mobilisierung der Wähler fördert, aber man darf nicht aus den Augen verlieren, dass es in der Regel nicht die Technologie ist, welche die Beteiligung der Bevölkerung auslöst, sondern der Wille der Behörden, die Bevölkerung wirklich teilhaben zu lassen und ihre Meinung zu berücksichtigen, aber auch die Fähigkeit, sie ernsthaft in den Entscheidungsprozess einzubeziehen. Das Problem der digitalen Kluft droht sich noch zuzuspitzen, denn es versteht sich von selbst, dass die Vervielfältigung der Online-Teilnahmeformen die Opfer dieser Kluft de facto ausschliesst.

Die digitale Revolution erhöht zudem die Gefahr einer «von Daten und Algorithmen diktierten Politik» (*Data-Driven Policy*) (die oft das neue Kleid der neoliberalen Expertokratie ist). Man muss deshalb zuerst **für eine gute Anwendung sorgen bzw. für eine Stärkung der Regeln, welche die demokratisch ernannten Entscheidungsträger gegen äussere Einflüsse schützt** (vgl. z.B. Art. 161 Abs. 2 BV: «Die Mitglieder der Bundesversammlung stimmen ohne Weisungen»). Aber es geht auch darum, dort, wo die Bevölkerung eine Kontrollmacht über das öffentliche Geschehen hat, die keine besonderen Kenntnissen (namentlich bei den politischen Rechten, z.B. Auszählen einer Abstimmung)

erfordert, **zu verhindern, dass diese Macht an Experten übertragen wird, weil es für das Verständnis des Funktionierens nun detailliertes Informatikwissen braucht**¹⁹⁰.

Art. 35 BV Verwirklichung der Grundrechte

Absatz 1 muss wie folgt angepasst werden: «Die Grundrechte müssen in der ganzen Rechtsordnung zur Geltung kommen, auch online.» Diese Änderung hätte zwar nur eine symbolische Wirkung, weil die aktuelle Formulierung vermutlich ausreicht, um das Ziel zu erreichen. Es scheint uns dennoch nicht unsinnig, darauf zu bestehen, vor allem nach der jüngsten Abstimmung über das Geldspielgesetz (die sich zwar nicht auf ein Grundrecht bezog, aber auf die Anwendung eines Verfassungsgrundsatzes), als einige Gegner versuchten, die Anwendung auf nicht-schweizerische Unternehmen zu bestreiten, die in unserem Land zugängliche Dienste anbieten.

Art. 38 BV Nationalität / Identität

Selbst wenn sich Art. 38 mit der Frage der Nationalität unter dem Gesichtspunkt der Zugehörigkeit zu einem Land und der Bedingungen ihrer Umsetzung befasst, sollte er auch die Grundlage dafür bilden, wie der Staat die Identität seiner Bürger und Einwohner anerkennt. Es wäre aber eingehender zu prüfen, ob Art. 38 der richtige Ort für diese Frage ist. Die Frage der digitalen Identität¹⁹¹ ist zu einer Schlüsselfrage geworden. Da geht es um die Pflicht, seine Kunden zu identifizieren (z. B. Abklärung des Alters), aber auch die Gefahr des Identitätsklaus und damit um Rechtssicherheit¹⁹². Die Identität seiner Bürger und Bewohner zu attestieren, ist eines der Vorrechte des Staates, das von der digitalen Revolution angegriffen wird¹⁹³. Die digitale Identität (e-ID) könnte nämlich teilweise privaten Unternehmen übertragen werden oder sich gar ausserhalb jeder staatlichen Kontrolle verselbständigen (z.B. beim Modell «*Self-Sovereign*» via Blockchain)¹⁹⁴. Es ist auch dafür zu sorgen, dass der Staat das Monopol über die Identifikation von juristischen Personen behält, ebenso wie ihrer wirtschaftlich Berechtigten.

Die unschöne Erfahrung des Lausanner Gemeinderats Xavier Company, den unter seinem richtigen Namen zu identifizieren FB sich lange weigerte (mit dem Argument, «Company» könnte zur Verwechslung mit einem Unternehmen führen...) zeigt, wie nötig es ist, Identifikationsfragen nicht Privaten zu überlassen.

Art. 43a BV Erfüllung staatlicher Aufgaben

Art. 43a ist so zu ergänzen, dass neue Leistungen und Infrastrukturen des Service public eingeführt und die öffentlichen Monopole in diesem Bereich gestärkt werden können.

Dieser neue digitale Service public muss Folgendes garantieren:

- **den allgemeinen Zugang zu den Netzwerken und ihr gutes Funktionieren;**
- **unerlässlich gewordene Online-Dienste und den Zugang zu ihnen.**

Neue Leistungen des digitalen Service public definieren

Zu den neuen Leistungen und Infrastrukturen des Service public, die durch die digitale Revolution nötig geworden sind, gehören:

- die **Netzneutralität**¹⁹⁵;
- die **Neutralität der Terminals**: ein gleichwertiger und universeller Zugang zu allen Daten auf allen Netzen reicht nicht, wenn die Terminals und Plattformen, die den Zugang ermöglichen, bestimmte Inhalte bevorzugen. So versuchen die GAFA mehr und mehr, die Suche im Internet an die Nutzung ihres Materials/ihrer

Hardware (oder ihrer Plattform) zu knüpfen, deren Anwendungsprogramme gesperrt sind, oder sie bieten diesen Zugang gratis an, um Kunden anzuziehen, die dann gebunden sind («Kindleisierung», abgeleitet vom Amazon-Leser «Kindle»). In den USA gehören die Leute mit solch eingeschränktem Zugang zu den benachteiligten sozialen Klassen!

- **Recht auf einen Internetzugang**, um die digitale Kluft aufzuheben. In Frankreich gibt es dieses Recht bereits auf Verfassungsebene als notwendige Bedingung für die Ausübung des Rechts auf «freie Meinungsäußerung», das durch die Menschenrechtserklärung¹⁹⁶ geschützt ist.
- **Recht auf einen leistungsfähigen Internetzugang auf dem ganzen Staatsgebiet.**
- Die Verwaltung von **Domainnamen und TLD** muss zum Service public gehören.

Im Übrigen muss der Zugang zu den Leistungen des Service public, einschliesslich jener von externalisierten öffentlichen Unternehmen, wirklich umfassend und nicht den Besitzern einer bestimmten Technologie vorbehalten sein, wie das kürzlich bei SBB-Kunden der Fall war, die über ein Smartphone der neuesten Generation verfügen mussten, um eine Entschädigung für die Bauarbeiten auf der SBB-Linie Bern – Lausanne im Sommer 2018 zu beantragen, was vor allem die Nutzer eines bestimmten Alters oder mit geringem Einkommen diskriminiert¹⁹⁷.

Die Vorrechte des Staats im «klassischen» Service public verteidigen

Doch die GAFA bieten laufend neue Dienste an, die so zentral werden, dass man sie als zum Service public gehörig betrachten muss. Sie setzen sich massiv in den Bereichen fest, die traditionell zum Service public gehören, sowohl bei den Leistungen (z.B. Kartographie, einst eine Kompetenz, die in den Bereich der nationalen Sicherheit gehörte!) als auch bei den Infrastrukturen. So verlegen FB, Google usw. eigene Unterwasserkabel¹⁹⁸. Die Planung solcher Infrastrukturen kann aber nur dann effizient und gerecht sein, wenn sie von der öffentlichen Hand gesteuert wird. Zum Beispiel gibt es in einigen Ländern einen Überfluss an Kabeln. In anderen hingegen, vor allem in Afrika, sind es zu wenige, um den Verkehr in Spitzenzeiten zu bewältigen ... und bei einem Defekt ist der ganze Verkehr unterbrochen. **Der Staat muss deshalb dafür sorgen, dass die Infrastrukturen des Service public in seiner Hand bleiben (zumindest bei der Planung).**

Neue Grundrechte:

Unsere Verfassung gewährt gewisse Rechte nicht, für die sich die Sozialdemokraten seit Jahrzehnten bzw. seit Beginn einsetzen. Keines ist neu, und ihre Notwendigkeit besteht nicht erst seit gestern. Aber die digitale Revolution macht deren Anerkennung umso dringender.

Recht auf digitale Bildung

Die Herausforderungen, vor welche die Bevölkerung durch die digitale Revolution gestellt wird, machen die Einrichtung eines Rechts auf Bildung, insbesondere digitale Bildung, und digitale Kultur (Digital Literacy) notwendiger denn je. Dies schliesst das **Recht auf Grundkenntnisse über das Funktionieren der Netze, über das Verstehen ihrer Inhalte (Fake News, Betrug, Scherze/Hoax, Satire, usw.), über die Folgen einer Online-Aktivität für Individuen und Umwelt** (z.B. die Teilnahme an Massen-Cyberbelästigung) **sowie über die darin versteckten Interessen** (z.B. wem welcher Dienst gehört) mit ein. Es ist auch unerlässlich, **die Aufklärung über die Rechte** (und Pflichten, z.B. Netiquette) zu verstärken. Diese Bildung muss ganz früh beginnen (Grundschule), und im Gegensatz dazu, was viele denken, hat gerade die junge Generation, die angeblich über das Internet alles weiss (die

«Millenials» und «Generation Y oder Z»), hier besonders viel Bedarf an Bildung.

Recht auf Weiterbildung

Das Recht auf Bildung muss auch ein Recht auf **digitale Weiterbildung** enthalten. Zunächst um trotz der rasanten technologischen Entwicklung die Chancen und Risiken erkennen zu können. Dann verlangt aber auch die Veränderung der Arbeitswelt die Schaffung eines echten **Rechts auf berufliche Weiterbildung und, gegebenenfalls, berufliche Wiedereingliederung**, nicht nur bei Stellenabbau infolge Digitalisierung. Diese berufliche Wiedereingliederung muss auch gewählt und geplant werden können (und nicht nur erduldet wegen der technologischen Entwicklung, die sich auf den Arbeitsplatz auswirkt), und sie muss durch die Sozialversicherungen und die Arbeitgeber (mit)finanziert werden.

Recht auf menschenwürdige Arbeit (inklusive gewerkschaftliche Freiheit gemäss Art. 28)

Die digitale Revolution ist sicher nicht der einzige Grund, der die Einrichtung eines **Rechts auf menschenwürdige Arbeit**¹⁹⁹ unerlässlich macht, aber sie führt zu neuen Verschlechterungen der Arbeitsbedingungen, was diese Notwendigkeit verstärkt, schon nur wegen des Aufkommens eines neuen Proletariats von «digitalen Sklaven» oder der Arbeitsplanung durch KI. Die Technologie muss Ausführende des Arbeiters sein und nicht umgekehrt!

Das Recht auf menschenwürdige Arbeit muss insbesondere garantieren:

- dass jeder Arbeiter über Rechte (selbst minimalste) verfügt, die ihm das Recht auf Arbeit einräumen, auch wenn er für eine Plattform arbeitet, die sich nicht als seine Arbeitgeberin versteht;
- dass jeder Arbeiter geschützt ist gegen die Folgen einer Arbeit, die ihn mit unerträglichen Inhalten (z.B. die Moderatoren von Videos mit Bildern extremer Gewalt, Kinderpornografie usw.) in Kontakt bringt;
- dass jeder Arbeiter geschützt ist gegen eine Rückkehr der extremen Unsicherheit, die eine Arbeit auf Abruf zur Folge hat, abhängig von der Willkür des Arbeitgebers, nicht nur im digitalen Bereich²⁰⁰;
- dass jeder Arbeiter einen würdigen Lohn erhält und dass er selbst bei Akkordarbeit ein solches Einkommen erzielen kann, wenn er der Arbeit den normalen Zeitaufwand widmet (also: jede Aufgabe, selbst die kleinste und unbedeutendste wie bei Amazons Mechanical Turk, muss korrekt entlohnt werden, damit die in einem Tag zu erledigenden Aufgaben ermöglichen, ein angemessenes Einkommen zu erzielen);
- dass jeder Arbeiter geschützt ist gegen Lohndumping und exzessive Konkurrenz, auch gegen Arbeiter, die im gleichen Unternehmen beschäftigt sind (inklusive Plattformen);
- dass die Zusammenarbeit mit Robotern und KI die Grundrechte des Arbeiters am Arbeitsplatz – insbesondere jenes, nicht ihrem Befehl unterstellt zu werden – bzw. bei einem Anstellungsgespräch respektiert, das von einem Roboter, KI oder einem Avatar (wie beim Digital Room von Manpower) geführt wird;
- dass ein Arbeiter, der mit einer intelligenten Maschine zusammenarbeitet, nicht für deren Fehler²⁰¹ verantwortlich gemacht wird;
- dass es keine Pflicht gibt, sich «erweitern» zu lassen, auch wenn es um die Ausführung von gefährlichen Arbeiten geht;
- dass jeder Arbeiter die Freiheit hat, sich einer Gewerkschaft anzuschliessen und eine Kontrolle (durch den Staat oder die Sozialpartner) seiner Arbeitsbedingungen vorzunehmen, auch wenn die Arbeitsplätze sehr dezentral sind (z.B. bei Telearbeit);

- dass das Recht, offline zu sein und sich gegen eine Überflutung durch neue Technologien (z.B. durch E-Mail-Flut²⁰²) wehren zu dürfen, präzisiert wird. Handkehrum müssen die Arbeitgeber gezwungen werden, neue Technologien einzusetzen, wenn dies ermöglicht, die Persönlichkeit ihrer Arbeiter besser zu schützen (z. B. die Verwaltung von E-Mails oder Kundenwünschen);
- dass die Arbeiter geschützt sind gegen die negativen Folgen des Trends, alle Leistungen zu bewerten²⁰³.

Schliesslich soll die Schweiz dort, **wo die digitale Revolution dies nötig macht, eine Stärkung der ILO-Übereinkommen initiieren** (und daran mitarbeiten), und selbstverständlich soll sie allfällige zukünftige Übereinkommen ratifizieren.

* * *

Abkürzungen

ARCEP	Autorité de régulation des communications électroniques et des postes (Frankreich)
BG	Bundesgericht
BR	Bundesrat
BV	Bundesverfassung, SR 101
CNNum	Conseil National du Numérique (Frankreich)
DSG	Bundesgesetz über den Datenschutz (E-DSG = Entwurf für ein neues DSG, gegenwärtig im eidgenössischen Parlament in Beratung)
DSGVO	Datenschutz-Grundverordnung (der EU) (2018)
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention), SR 0.101
FB	Facebook
F&E	Forschung und Entwicklung
GAFA	Google (Alphabet), Apple, Facebook, Amazon. Das (manchmal durch M für Microsoft ergänzte) Akronym bezeichnet im vorliegenden Dokument alle «Internetriesen» des Silicon Valley, inklusive weitere dominante Firmen wie PayPal, TripAdvisor, Airbnb, Booking.com, Uber usw. sowie ihre chinesischen Konkurrenten wie Alibaba, Baidu, Tencent oder WeChat.
ILO	Internationale Arbeitsorganisation
KG	Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen, SR 251.
KI	Künstliche Intelligenz
MIT	<i>Massachusset Institute of Technology</i>
M2M	<i>Machine-to-Machine</i> : Vernetzte Objekte, die untereinander Informationen austauschen.
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
P2P	<i>Peer-to-Peer</i>
QS	<i>Quantified Self</i> : Selbstvermessung
SGB	Schweizerischer Gewerkschaftsbund
SR	Systematische Rechtssammlung des Schweizer Bundesrechts
TLD	<i>Top Level Domain</i> : Höchste Ebene des Domain-Namens. Bsp.: «.ch», «.biz», «.swiss».

VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
ZGB	Zivilgesetzbuch, SR 210

Bibliografie

Ohne gegenteilige Anmerkung werden die Quellen nur mit dem Namen des ersten aufgeführten Autors zitiert. Alle Webseiten wurden in den Monaten Juni und Juli 2018 abgerufen.

- Acemoglu, Daron/Restrepo, Pascual, (MIT) Robots and Jobs: Evidence from US Labor Markets, Boston, März 2017, unter: <http://www.nber.org/papers/w23285>
- Article 19, Le droit à l’anonymat en ligne, document d’orientation, London, 2015.
- Attali, Jacques (Hg.), L’avenir du travail, Paris 2007.
- Autorité de régulation des communications électroniques et des postes (ARCEP), Smartphones, tablettes, assistants vocaux... Les maillons faibles de l’ouverture d’internet, Paris, Februar 2018.
- Avenir Suisse (Hg.), Wenn die Roboter kommen, Den Arbeitsmarkt für die Digitalisierung vorbereiten, Zürich, Oktober 2017.
- Bradley, Joseph/Barbier, Joel/Handler, Doug, L’internet of everything, un potentiel de 14,4 trillions de Dollars, Weissbuch herausgegeben von Cisco, 2013. https://www.cisco.com/web/FR/tomorrow-starts-here/pdf/ioe_economy_report_fr.pdf
- Brundage Miles (et al.), The malicious use of artificial intelligence: Forecasting, prevention and mitigation, Oxford, Februar 2018.
- Bundesrat, Auswirkungen der Digitalisierung auf Beschäftigung und Arbeitsbedingungen – Chancen und Risiken, Bericht in Erfüllung verschiedener parlamentarischer Eingaben, Bern, 8. November 2017.
- Conseil National du Numérique (CNNum), La libre circulation des données dans l’Union Européenne, Paris, April 2017.
- Crawford, Kate, Artificial Intelligence’s White Guy Problem, New York Times vom 25. Juni 2016.
- Cuvelliez, Charles, Légiférer contre les « fake news » ne sert à rien, Le Monde vom 4. April 2018.
- Degryse, Christophe, Les impacts sociaux de la digitalisation de l’économie, working paper 2016.02 de l’ETUI, Brüssel.
- Diakopoulos, Nicholas, Friedler, Sorelle, How to Hold Algorithms Accountable: Algorithmic systems have a way of making mistakes or leading to undesired consequences. Here are five principles to help technologists deal with that, MIT Technology Review, 17.11.2016.
- Doueïhi, Milad, Le numérique, un nouveau processus civilisateur, Le Monde vom 24. Januar 2018.
- Doweck, Gilles, Réseaux sociaux : « Les téléphones, les tablettes, les ordinateurs sont devenus des armes létales », Le Monde vom 29. Mai 2018, unter https://abonnes.lemonde.fr/idees/article/2018/05/29/reseaux-sociaux-les-telephones-les-tablettes-les-ordinateurs-sont-devenus-des-armes-letaales_5306266_3232.html
- Ehrenzeller/Schindler/Schweizer/Vallender, Die Schweizerische Bundesverfassung, St. Galler Kommentar, Zürich/St. Gallen 2014.
- Fichter, Adrienne, Rausgewunden, Stammtischpolterer in elegant: Wie Entscheidungsträger sich mit allerlei Floskeln um eine sinnvolle Debatte über

- Digitalisierung drücken – ein Erfahrungsbericht, publiziert am 18.1.2018 auf republik.ch: <https://www.republik.ch/2018/01/18/altfuersten> (abgerufen am 14.6.18).
- Flückiger, Alexandre, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ? AJP/PJA 2013, S. 837ff.
 - Forteza, Paula/Frassa Christophe-André, Proposition de « Charte du numérique » à l'attention des présidents de l'Assemblée nationale et du Sénat français, Paris, 21. Juni 2018.
 - Gallusser, Martin / Ringger, Beat (Denknetz), Cyborgs, Blockchains, künstliche Intelligenz: Was kommt da auf uns zu? Das Denknetz, 003/ April 2018, S. 14ff.
 - Gencer, Adem Efe (et al.), Decentralization in Bitcoin and Ethereum, Cornell University Library, März 2018 (Zusammenfassung unter: <http://hackingdistributed.com/2018/01/15/decentralization-bitcoin-ethereum/>).
 - Honsell, Heinrich/Isenring, Bernhard/Kessler, Martin, Schweizerisches Haftpflichtrecht, Zürich/Basel/Genf, 2013.
 - Ito, Joichi, Resisting Reduction, Designing our Complex Future with Machines, a manifesto, 14.11.2017 unter <https://jods.mitpress.mit.edu/pub/resisting-reduction>
 - Jaccard, Gabriel, Partie I : L'identité digitale et la création du surhomme 2.0, Jusletter vom 30. April 2018.
 - Kerdellant, Christine, Dans la Google du Loup, Paris (Plon), 2017.
 - Kitano, Naho, Animism, Rinri, Modernization: the Base of Japanese Robotics, unter: <http://www.roboethics.org/icra2007/contributions/KITANO%20Animism%20Rinri%20Modernization%20the%20Base%20of%20Japanese%20Robo.pdf>.
 - Lampart, Daniel/Cirigliano, Luca, Digitalisierung muss den Berufstätigen nützen: Analyse und Handlungsbedarf, Dossier des SGB, Oktober 2017.
 - Lohmann, Melinda, Ein europäisches Roboterrecht – überfällig oder überflüssig? ZRP 6/2017, S. 168ff.
 - Lohr, Steve, Data-ism ,The revolution transforming decision making, consumer behavior, and almost everything else, New York, 2015.
 - Lorenzi, Jean-Hervé/Berrebi, Mickaël, L'avenir de notre liberté. Faut-il démanteler Google ?, Paris (Eyrolles) 2017.
 - Maas, Heiko, Internet-Charta: Unsere digitalen Grundrechte, Die Zeit, 10. Dezember 2015.
 - Morin-Desailly, Catherine, L'Union européenne, colonie numérique ? Rapport d'information fait au nom de la commission des affaires européennes, 2013.
 - Morozov, Evgeny, silicon circus, blog unter: <https://blog.mondediplo.net/-Silicon-circus->
 - Nevejans, Nathalie, Règles européennes de droit civil en robotique, étude pour la commission juridique du Parlement européen, Brüssel 2016.
 - OECD, Automation, Skills use and Training, Social – Employment and Migration Working Paper Nr. 202, Paris, 2018, unter: <https://www.oecd-ilibrary.org/docserver/2e2f4eea-en.pdf?expires=1529935558&id=id&accname=guest&checksum=FF242B48771C2257167E7936E9DBEC75>.
 - Oftinger, Karl/Stark, Emil, Schweizerisches Haftpflichtrecht, Zürich 1995
 - Perry Barlow, John, A Declaration of the Independence of Cyberspace, 8. Februar 1996 und Ertzscheid, Olivier, Une nouvelle déclaration d'indépendance du cyberspace, Libération vom 9. Februar 2018.
 - Rifkin, Jeremy, La nouvelle société du coût marginal zéro, Paris 2014.

- Rossnagel, Alexander, Eine Zukunft ohne Selbstbestimmung? in: Spektrum Kompakt, Der Digitale Mensch, 4.10.2016, S. 41f.
- Rouvroy, Antoinette, Des données et des hommes, Droits et libertés fondamentales dans un monde de données massives, Rapport à destination du Comité Consultatif de la Convention pour la protection des personnes au regard du traitement automatisé de données personnelles du Conseil de l'Europe, Strassburg, 11. Januar 2016 (zitiert als: Rouvroy, données).
- Rouvroy, Antoinette, Le gouvernement algorithmique ou l'art de ne pas changer le monde, La revue nouvelle, 8/2016 und überarbeitete Version unter https://www.academia.edu/28370856/Le_gouvernement_algorithmique_ou_lart_de_ne_pas_changer_le_monde (zitiert als: Rouvroy, algorithmes).
- Rouvroy, Antoinette, La transparence des algorithmes : un leurre ? Publiziert am 4. März 2016 unter <https://www.linkedin.com/pulse/la-transparence-des-algorithmes-un-leurre-antoinette-rouvroy/> (zitiert als: Rouvroy, transparence).
- Schwaab, Jean Christophe, La licéité de l'évaluation et du « forced ranking » en droit suisse du travail, in Dunand/Mahon (Hg.), La protection des données dans les relations de travail, Genf/Zürich/Basel, 2017.
- SP Schweiz, Internetpolitik, Die Chancen des Internets sollen Allen zu Gute kommen und nicht nur einigen Wenigen: Positionspapier verabschiedet an der DV in St. Gallen vom 5. Dezember 2015.
- von Stockar, Thomas (et al.), Sharing economy – teilen statt besitzen, TA-Swiss, Zürich 2018, abrufbar hier: https://vdf.ch/index.php?route=product/product/download&ea_id=9123&product_id=2090.
- Thiel, Peter, De zéro à un, Comment construire le futur, Paris (JC Lattès) 2016.
- Ulmi, Nic, L'apprentissage de l'incertitude, «Horizons» vom 5. Juni 2018, unter: <https://www.revue-horizons.ch/2018/06/05/lapprentissage-de-lincertitude/> (abgerufen am 18. Juni 2018).
- VBS, Nationale Strategie zum Schutz vor Cyber-Risiken, Bern 2012.
- Villani, Cédric, Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne, rapport de mission parlementaire, März 2018.
- Wachter-Boettcher, Sara, Technically Wrong: Sexist Apps, Biased Algorithms, and other threats of toxic tech, New York, 2017.
- Widmer, Michael/Hegy, Stefan, Ethische Normen und Werte im Zeiten von Quantified Self, Jusletter vom 5. Februar 2018.
- Wildhaber, Isabelle, Die Roboter kommen, Konsequenzen für Arbeit und Arbeitsrecht, ZSR 2016 I S. 315ff.
- Wolfangel, Eva, Wie sichern wir unsere Unberechenbarkeit? in: Spektrum Kompakt, Der Digitale Mensch, 4.10.2016, S. 69ff.
- Wohlmann, Herbert, Das struktur- und gesellschaftspolitische Versagen des Kartellrechts, Jusletter vom 23. April 2018.

Anmerkungen und Verweise:

- ¹ Vgl. Die historische Zusammenfassung von Gallusser/Ringger, S. 15, oder die Einleitung von Degryse, S. 9.
- ² https://www.republik.ch/2018/06/25/weltweite-webkunst?utm_source=newsletter&utm_medium=email&utm_campaign=republik%2Fnewsletter-editorial-250618. Der Larousse definiert Algorithmen folgendermassen: «Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur.» Algorithmen sind nicht zwingend digital (vgl. obiges Beispiel des Webstuhls von Jacquard): Auch Kochrezepte und klinische Befunde sind Algorithmen.
- ³ Rouvroy, données, S. 5ff.
- ⁴ Gallusser/Ringger, S. 19, Degryse, S. 9
- ⁵ https://www.lemonde.fr/europe/article/2011/08/08/emeutes-a-londres-la-presse-britannique-dramatise-et-tente-de-comprendre_1557250_3214.html
- ⁶ Fichter
- ⁷ Villani, S. 105
- ⁸ BR, S. 105
- ⁹ Degryse, S. 12
- ¹⁰ Nr. 380 Juni 2018, S. 43
- ¹¹ BR, S. 104
- ¹² Villani, S. 124, mit zahlreichen Beispielen. Villani unterstreicht jedoch das Risiko des «Rebound-Effekts».
- ¹³ Siehe das Beispiel des Wassermanagements und der Optimierung der Bewässerung in einem tunesischen Olivenhain unter https://abonnes.lemonde.fr/afrique/article/2018/06/22/en-tunisie-un-algorithme-met-de-l-huile-dans-les-systemes-d-irrigation_5319533_3212.html
- ¹⁴ Villani, S. 130f. mit zahlreichen Beispielen
- ¹⁵ Villani, S. 127-128. Zum Mooreschen Gesetz: https://de.wikipedia.org/wiki/Mooresches_Gesetz
- ¹⁶ Widmer/Hegi, Rz 5
- ¹⁷ Villani, S. 195
- ¹⁸ Denknnetz 003/April 2018, S. 26f.
- ¹⁹ Villani, S. 173
- ²⁰ Jaccard, N 70-71, 76. Siehe auch « L'Estonie, première cybervictime de Moscou » https://abonnes.lemonde.fr/international/article/2017/03/14/l-estonie-premiere-cybervictime-de-moscou_5093948_3210.html
- ²¹ Von Degryse zitierte Verweise, S. 9f., BR, S. 104
- ²² « Le progrès technique est-il toujours source de croissance ? », Alternatives Economiques Nr. 376, Februar 2018, S. 78f.
- ²³ Die es seit Ewigkeiten gibt, woran Gallusser/Ringger, S. 19 zurecht erinnern... Zu diesem Thema wären die sehr detaillierte Studie von von Stockar, S. 137ff. und die zitierten Verweise zu lesen.
- ²⁴ Selbst wenn die Wirkung der Sharing economy auf die Umwelt unsicher ist, vgl. von Stockar, S. 148ff.
- ²⁵ Vgl. das Interview von Hugues Sibille, Präsident des Labo de l'économie sociale et solidaire, in «Nouvelobs»: <https://www.nouvelobs.com/rue89/rue89-le-grand-entretien/20160826.RUE1450/l-economie-collaborative-accroit-les-inegalites-patrimoniales.html>. Vgl. auch Degryse, S. 30ff und 51ff.
- ²⁶ Degryse, S. 49.
- ²⁷ Zitiert von Degryse, S. 49.
- ²⁸ Villani, S. 101; Interview von David Dorn in La vie économique 1-2/2018, S. 47ff.
- ²⁹ Alternatives Economiques Nr. 380 Juni 2018, S. 42, sowie: <https://www.numerama.com/politique/245152-selon-le-mit-chaque-robot-introduit-sur-le-marche-du-travail-detruit-6-emplois.html> und <https://www.numerama.com/tech/340505-finalement-les-robots-ne-vont-pas-nous-voler-tout-notre-travail.html>
- ³⁰ Zitiert in Degryse, S. 13 und 26
- ³¹ Degryse, S. 13f., S. 32ff.
- ³² Degryse S. 21f. und die zitierten Verweise
- ³³ Degryse, S. 43
- ³⁴ Schwaab
- ³⁵ BR, S. 105. Siehe auch: https://abonnes.lemonde.fr/emploi/article/2018/07/01/numerique-la-nouvelle-fracture-sociale_5324053_1698637.html
- ³⁶ BR, S. 105
- ³⁷ Degryse, S. 40ff.

-
- ³⁸ Von Stockar, S. 147 und die zitierten Verweise
- ³⁹ Degryse und die zitierten Verweise, S. 24, 38f.
- ⁴⁰ Degryse, S. 50. Siehe auch: https://abonnes.lemonde.fr/emploi/article/2018/07/01/numerique-la-nouvelle-fracture-sociale_5324053_1698637.html
- ⁴¹ Vgl. zum Beispiel diesen Bericht einer französischen «Transkribiererin» der Sprachassistentin Cortana (Microsoft) https://www.laquadrature.net/fr/temoin_cortana
- ⁴² Degryse und die zitierten Verweise, S. 9ff. und S. 50
- ⁴³ <http://moralmachine.mit.edu/hl/fr>
- ⁴⁴ Rossnagel, S. 48
- ⁴⁵ Vgl. beispielsweise: Naomi Klein, La stratégie du choc, La montée d'un capitalisme du désastre, Paris 2013.
- ⁴⁶ Und damit das Wesentliche des Arbeitsvertrags, das heisst die Bezahlung durch den Arbeitgeber der vom Arbeiter in seinem Dienst verbrachten Zeit.
- ⁴⁷ Avenir.Suisse. Der BR, S. 105, spricht euphemistisch von «neuen Erwerbchancen durch innovative Geschäftsmodelle und flexiblere Arbeitsbedingungen»
- ⁴⁸ Gallusser/Ringger, S. 18
- ⁴⁹ <https://blog.mondediplo.net/2017-12-13-Le-taylorisme-a-la-mode-hippie>
- ⁵⁰ Wie das Beispiel der Entschädigung der SBB-Kunden für die Arbeiten auf der Linie nach Bern im Sommer 2018 zeigt: <http://www.rts.ch/info/suisse/9712679-defaillante-discriminante-l-application-d-indemnisiation-des-cff-critiquee.html>
- ⁵¹ SP, S. 2
- ⁵² Villani, S. 176, von Stockar, S. 146f.
- ⁵³ Von Stockar, S. 99
- ⁵⁴ Degryse, S. 48
- ⁵⁵ Crawford, Villani, S. 163ff. Vgl. auch <https://www.tagesanzeiger.ch/sonntagszeitung/itentwickler-sind-auch-nur-maenner/story/22557041> mit zahlreichen Beispielen.
- ⁵⁶ BR, S. 105
- ⁵⁷ BGE 143 V 21; BG-Entscheide 1B_185/2016, 1B_186/2016 und 1B_188/2016 vom 16.11.2016 (Facebook) sowie 1B_142/2016 vom 16.11.2016 (Google/Gmail). Vgl. auch die Motion 18.3379 der RK-S sowie die Motionen Levrat 16.4082 und Schwaab 16.4080, die ihr zugrunde liegen.
- ⁵⁸ <https://www.24heures.ch/high-tech/facebook-debloque-contacts-erreur/story/24295694>
- ⁵⁹ Rossnagel, S. 45
- ⁶⁰ <https://www.theguardian.com/news/2017/may/22/how-facebook-allows-users-to-post-footage-of-children-being-bullied>. Alle von «The Guardian» zu Facebook gesammelten Dokumente finden sich hier: <https://www.theguardian.com/news/series/facebook-files>. Siehe auch dieses Dokument, das die internen Regeln von FB zeigt, um die Nutzer zu «verbannen»: https://motherboard.vice.com/en_us/article/ne5nxz/leaked-documents-facebook-threshold-delete-pages-groups
- ⁶¹ <https://www.watson.ch/!5314555>
- ⁶² Das ist zum Beispiel beim indischen Premierminister Narendra Modi oder beim Tesla-Besitzer Elon Musk der Fall, <https://www.rts.ch/info/monde/9605595-les-fans-d-elon-musk-ne-semblent-plus-tolerer-la-moindre-critique-contre-lui.html>
- ⁶³ VBS, Nationale Strategie, S. 11, Rossnagel.
- ⁶⁴ Was jedoch den Bundesrat in seiner Antwort auf die Interpellation 17.3277 nicht zu beunruhigen scheint.
- ⁶⁵ Widmer/Hegyí, N 27f.
- ⁶⁶ Rouvroy, données, S. 44, der von «konstitutiver Normativität» spricht.
- ⁶⁷ So nutzt der australische Zolldienst ein von IBM entwickeltes System, welches das «Terror-Risiko» ausländischer Passagiere, die in das Land fliegen wollen, analysiert, Villani, S. 149.
- ⁶⁸ Rouvroy, données, S. 18ff., 30f.
- ⁶⁹ Honsell/Isenring/Kessler, S. 5, Oftinger/Stark, S. 12
- ⁷⁰ Rouvroy, algorithmes
- ⁷¹ Siehe z. B. dieses aufschlussreiche Beispiel: <http://www.wired.co.uk/article/uber-employment-lawsuit-gig-economy-leigh-day>
- ⁷² Rouvroy, données, S. 45
- ⁷³ Sonntagszeitung vom 14.12.2014
- ⁷⁴ Siehe auch Mascha Madörins Beispiel eines jungen Diabetespatienten in Denknetz 003/April 2018, S. 27f.).
- ⁷⁵ Crawford
- ⁷⁶ Rouvroy, algorithmes/données, S. 45
- ⁷⁷ Villani, S. 150
- ⁷⁸ Brundage et al.
- ⁷⁹ https://abonnes.lemonde.fr/idees/article/2018/05/28/parcoursup-pourquoi-un-tel-choc_5305731_3232.html

-
- ⁸⁰ https://abonnes.lemonde.fr/societe/article/2018/06/02/les-lyceens-de-banlieue-et-les-embuches-de-parcoursup_5308639_3224.html?xtmc=parcoursup&xtcr=5
- ⁸¹ <https://www.alternatives-economiques.fr/boursiers-parcoursup-enterine-discrimination-sociale/00085018>
- ⁸² Carnegie-Mellon zitiert in The Guardian <https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study>
- ⁸³ <https://www.srf.ch/news/schweiz/rueckfallrisiko-bei-straftaetern-die-grosse-screening-maschine>
- ⁸⁴ Wachter-Boettcher, siehe auch sein Interview in «Watson» auf <https://www.watson.ch/digital/leben/156143365-warum-siri-es-lustig-findet-wenn-du-ihr-von-deiner-vergewaltigung-erzaehlst>
- ⁸⁵ <https://www.tagesanzeiger.ch/sonntagszeitung/itentwickler-sind-auch-nur-maenner/story/22557041>
- ⁸⁶ Wachter-Boettcher, siehe auch sein Interview in «Watson» auf <https://www.watson.ch/digital/leben/156143365-warum-siri-es-lustig-findet-wenn-du-ihr-von-deiner-vergewaltigung-erzaehlst>
- ⁸⁷ https://abonnes.lemonde.fr/pixels/article/2018/06/27/epingle-pour-biais-raciste-microsoft-modifie-son-logiciel-de-reconnaissance-faciale_5321958_4408996.html
- ⁸⁸ Vgl. auch die rassistische Tendenz der Gesichtserkennungssoftware «Face API» in der vorherigen Anmerkung, die auf einer Programmier-Datenbank mit Gesichtern vor allem von weissen Männern beruht.
- ⁸⁹ Gallusser/Ringger, S. 17, Degryse, S. 52, Rouvroy, algorithmes. Die Ansteckungswirkung funktioniert auch in der anderen Richtung, insofern gewisse Algorithmen der Solvenzbewertung zum Schluss kommen, dass «gute Menschen sich miteinander verbinden»: <https://www.journaldunet.com/ebusiness/le-net/1127850-attention-a-vos-amis-facebook-ils-pourraient-vous-couter-votre-pret/>
- ⁹⁰ Rouvroy, algorithmes, der sogar von «algorithmischen Diktaturen» spricht.
- ⁹¹ Villani, S. 28
- ⁹² Rouvroy, données. S. 25
- ⁹³ Rouvroy, données, S. 28ff.
- ⁹⁴ Experiment des MIT, zitiert in Rouvroy, données, S. 28
- ⁹⁵ Rouvroy, données, S. 28
- ⁹⁶ Eine unter <http://www.tilllate.com/fr/story/donn%C3%A9es-facebook?ref=home-story-3> erschienene Analyse der von FB gespeicherten Daten zeigt, dass deren Wissen über die User sehr präzise ist, selbst wenn sie lügen; FB hat zum Beispiel das Geschlecht eines Mannes bestimmen können, der sich als Frau ausgab.
- ⁹⁷ Widmer/Hegyí, Rz 29
- ⁹⁸ Interview in «20 Minuten» vom 19.8.14
- ⁹⁹ Villani, S. 123
- ¹⁰⁰ https://www.lemonde.fr/technologies/article/2009/01/12/une-recherche-google-a-un-cout-energetique_1140651_651865.html
- ¹⁰¹ Bilan vom 4. Juli 2018, S. 16f.
- ¹⁰² https://www.courrierinternational.com/article/desole-la-voiture-autonome-ne-mettra-pas-fin-aux-embouteillages?utm_term=Autofeed&utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter&Echobox=1530451622. Siehe auch den Artikel zum Niedergang des öffentlichen Verkehrs in zahlreichen Städten entwickelter Länder, weil deren Nutzer mehr und mehr Über nutzen: <https://www.economist.com/international/2018/06/23/public-transport-is-in-decline-in-many-wealthy-cities?fsrc=scn/tw/te/bl/ed/publictransportisindeclineinmanywealthycitiesmissingthebus>
- ¹⁰³ Google beherrscht z. B. 91,6% des Weltmarkts in Onlinesuche, gemäss statcounter.com, zitiert in Gallusser/Ringger, S. 24
- ¹⁰⁴ Gallusser/Ringger, S. 18, Rouvroy, données, S. 6
- ¹⁰⁵ von Stockar, S. 140f.
- ¹⁰⁶ Villani, S. 29, der namentlich das Beispiel von Netflix angibt, wo einer der Leiter gesteht, dass eine Internalisierung der Entwickler, welche die Inhouse-API nutzen, fast eine Milliarde USD pro Jahr kosten würde.
- ¹⁰⁷ Vgl. «Fermeture de BuzzFeed France : quel modèle économique pour les médias en ligne ?», unter https://abonnes.lemonde.fr/actualite-medias/live/2018/06/08/fermeture-de-buzzfeed-france-quel-modele-economique-pour-les-medias-en-ligne_5311624_3236.html.
- ¹⁰⁸ Gemäss Gencer et al. kontrollieren die 4 grössten Bitcoin-Schürfer bzw. die 3 grössten Ethereum-Schürfer 50% ihrer jeweiligen Blockchains.
- ¹⁰⁹ <https://www.watson.ch/!100008372>
- ¹¹⁰ Vgl. den Fall eines Luzerner Restaurateurs unter <https://www.watson.ch/!833465447>, aber auch diese Beispiele: <https://www.watson.ch/!145590740> (Influencerin, die im «Austausch» mit positiven Kommentaren Gratisleistungen fordert) und <https://www.numerama.com/business/333246-lufc-victime-dun-review-bombing-des-opticiens-ou-comment-les-notes-sur-internet-cristallisent-les-passions.html> (ein Berufsverband von Optikern, die versuchen, den Ruf eines Konsumentenverbandes auf FB zu untergraben).

-
- ¹¹¹ La Vie économique, 3/2018, S. 36
- ¹¹² <https://www.journaldunet.com/ebusiness/le-net/1127850-attention-a-vos-amis-facebook-ils-pourraient-vous-couter-votre-pret/>
- ¹¹³ Wohlmann.
- ¹¹⁴ Morozov, <https://blog.mondediplo.net/2018-04-10-Pour-un-service-public-des-donnees>
- ¹¹⁵ Alternatives économiques Nr. 379, Mai 2018
- ¹¹⁶ Man muss sich jedoch bewusst sein, dass die Linke, die Gewerkschaften und die sozialen Bewegungen mit dieser Art von massiven Interventionen in den sozialen Netzwerken im Stil von «Agitprop» oder «Name and shame», namentlich unter Nutzung von Werkzeugen wie «Thunderclap», durchaus vertraut sind...
- ¹¹⁷ Doweck
- ¹¹⁸ https://abonnes.lemonde.fr/pixels/article/2018/07/09/planebae-la-belle-rencontre-dans-un-avion-vire-au-cauchemar-pour-la-vie-privee_5328419_4408996.html?xtmc=planebae&xtcr=1
- ¹¹⁹ Vgl. das jüngste Beispiel der Operateurinnen der französischen Notfalldienste, die zu Unrecht für den Tod einer jungen Frau verantwortlich gemacht wurden, deren Hilferuf nicht ernst genommen wurde: http://abonnes.lemonde.fr/les-decodeurs/article/2018/05/14/affaire-naomi-trois-operatrices-du-samu-mises-en-cause-a-tort-victimes-de-harcelement_5298898_4355770.html?xtmc=naomi_harcelement&xtcr=1
- ¹²⁰ VBS, S. 13ff.
- ¹²¹ Rouvroy, algorithmes
- ¹²² Verweise zitiert in Degryse S. 9f.
- ¹²³ Rouvroy, données, S. 13f.
- ¹²⁴ Rouvroy, algorithmes
- ¹²⁵ Wolfangel, S. 74
- ¹²⁶ <http://www.sciencemag.org/news/2018/05/ai-researchers-allege-machine-learning-alchemy>
- ¹²⁷ Alternatives Economiques Nr. 380 Juni 2018
- ¹²⁸ Gallusser/Ringger, S.23
- ¹²⁹ Rossnagel
- ¹³⁰ Rossnagel
- ¹³¹ Alternatives économiques, Nr. 377, März 2018
- ¹³² Lorenzi/Berrebi
- ¹³³ Gallusser/Ringger, S. 19
- ¹³⁴ Das heisst die Fähigkeit, die Natur zu beobachten und zu studieren und sie nachher zu reproduzieren – eine Maschine wird z. B. unfähig sein zu begreifen, weshalb eine Ameise das x-fache ihres Eigengewichts tragen kann
- ¹³⁵ Fortezza/Frassa, vgl. https://abonnes.lemonde.fr/pixels/article/2018/06/22/comment-des-parlementaires-veulent-inscrire-la-neutralite-du-net-dans-la-constitution-francaise_5319402_4408996.html
- ¹³⁶ Morin-Desailly in Bezug auf Frankreich, aber die Feststellung gilt für ganz Europa.
- ¹³⁷ Vgl. auch Maas, Art. 12
- ¹³⁸ Gallusser/Ringger, S. 18
- ¹³⁹ Widmer/Hegyí, Rz 36ss, Rouvroy, algorithmes.
- ¹⁴⁰ Villani, S. 142f
- ¹⁴¹ Ausgeführt vor allem bei Rouvroy, données, S. 51, Diakopoulos/Friedler et Villani, S. 146ff. (*Transparency by design, Ethics by design, Discrimination impact assesment*). Siehe auch das Postulat Marti (Schwaab) 16.4007.
- ¹⁴² Lohmann, Villani, S. 140ff; vgl. auch Art. 15.1 DSGVO
- ¹⁴³ <http://ingenuingenieur.blog.lemonde.fr/2018/05/22/que-revele-une-premiere-analyse-du-code-source-de-parcoursup/>
- ¹⁴⁴ Rouvroy, transparence
- ¹⁴⁵ « Qui est responsable en cas d'accident impliquant une voiture autonome ? » in Le Monde vom 20. März 2018.
- ¹⁴⁶ Jaccard, Rz 82ff.
- ¹⁴⁷ Jaccard, Rz 92ff.
- ¹⁴⁸ Vgl. « Le terrifiant assistant de Google qui appelle le coiffeur à votre place »: https://abonnes.lemonde.fr/pixels/article/2018/05/16/le-terrifiant-assistant-google-qui-appelle-le-coiffeur-a-votre-place_5299701_4408996.html?xtmc=le_terrifiant_assistant_google&xtcr=1
- ¹⁴⁹ Madörin in Denknetz 003/April 2018, S. 27
- ¹⁵⁰ Kitano
- ¹⁵¹ Nevejans, Kapitel 4 und die zitierten Verweise
- ¹⁵² Degryse, S. 43
- ¹⁵³ Wildhaber, S. 217ff.

-
- ¹⁵⁴ Maas, Art. 4
- ¹⁵⁵ Man denke etwa an die Frage von Leben und Tod im Zusammenhang mit dem Einsatz von «Killerrobotern». Vgl. auch Villani, S. 152.
- ¹⁵⁶ Villani, S. 29, 152; vgl. auch Art. 22 DSGVO.
- ¹⁵⁷ Wolfangel, S. 70.
- ¹⁵⁸ Rouvroy, données, S. 49f.
- ¹⁵⁹ CourEDH: Huch Jordan vs. UK vom 4. Mai 2001 24746/94, Kemalaloglu vs. Türkei, 19986/06 (2012), N.34s.; BGE 131 I 455 c. 1.2.5 et 135 I 113 c. 2.1; Schweizer in Ehrenzeller/Schindler/Schweizer/Vallender S. 305ff. und die darin zitierten Verweise.
- ¹⁶⁰ Ein Beispiel unter vielen ist die traurige Berühmtheit des «forum 18-25» von jeuxvideo.com, das vor allem dazu diente, digitale Massenangriffe gegen militante Feministinnen zu organisieren <https://www.numerama.com/politique/222533-cyber-harcelement-sur-le-18-25-jeuxvideo-com-pourra-t-il-se-sauver-de-sa-communaute.html>, manchmal von Erfolg gekrönt: <https://www.numerama.com/politique/302215-le-06-anti-relous-desactive-apres-une-attaque-du-forum-18-25-de-jeuxvideo-com.html>
- ¹⁶¹ Vgl. #PlaneBae : https://abonnes.lemonde.fr/pixels/article/2018/07/09/planebae-la-belle-rencontre-dans-un-avion-vire-au-cauchemar-pour-la-vie-privee_5328419_4408996.html?xtmc=planebae&xtcr=1
- ¹⁶² Zu den in Frankreich ergriffenen Massnahmen: https://abonnes.lemonde.fr/pixels/article/2018/05/17/l-assemblee-nationale-muscule-les-sanctions-contre-le-cyberharcelement-de-groupe_5300473_4408996.html?xtmc=cyberharcelement&xtcr=1
- ¹⁶³ Maas, Art. 13
- ¹⁶⁴ Gegenbeispiel: die Entschädigung von SBB-Kunden für die Bauarbeiten auf der Strecke Bern – Lausanne im Sommer 2018, für welche die Kunden zwingend eine App verwenden mussten, die nur auf den neuesten Smartphones lief: <http://www.rts.ch/info/suisse/9712679-defaillante-discriminante-l-application-d-indemnisiation-des-cff-critiquee.html>
- ¹⁶⁵ Siehe die Beispiele von Youtuber-Eltern in den USA, denen die Sorge über ihre Kinder entzogen wurde und die aus den sozialen Medien verbannt wurden: <https://www.numerama.com/pop-culture/395780-aux-etats-unis-youtube-bannit-des-parents-qui-ont-piege-leurs-enfants.html>
- ¹⁶⁶ Beispiele auf: https://www.lemonde.fr/pixels/article/2018/05/26/ufs-surprises-deballages-et-comptines-sur-youtube-le-tunnel-des-videos-pour-enfants_5305043_4408996.html
- ¹⁶⁷ CNNum
- ¹⁶⁸ Villani, S. 37
- ¹⁶⁹ https://abonnes.lemonde.fr/pixels/article/2018/05/25/une-enceinte-connectee-d-amazon-envoie-une-conversation-privee-par-erreur_5304453_4408996.html Vgl. auch die Geschichte einer Angestellten, die an der Entwicklung der Stimmassistentin Cortana (Microsoft) beteiligt war; sie berichtet von zahlreichen «irrtümlichen» Aufzeichnungen ohne Wissen des Users: https://www.laquadrature.net/fr/temoin_cortana
- ¹⁷⁰ Maas, Art. 11
- ¹⁷¹ Minderheit in der Lehre, vgl. Flückiger, S. 847f.
- ¹⁷² Vgl. die parlamentarische Initiative Vischer 14.413. Flückiger, S. 851ff. PSS, F. 11f.
- ¹⁷³ PSS, S. 12f., Artikel 19, S. 2f.
- ¹⁷⁴ Rouvroy, données, S. 28ff.
- ¹⁷⁵ Villani, S. 148ff.
- ¹⁷⁶ CNNum, Gallusser/Ringger, S. 17, Villani, S. 30ff., 130ff. 196.
- ¹⁷⁷ <https://blog.mondediplo.net/2016-12-15-Pour-un-populisme-numerique-de-gauche> und <https://blog.mondediplo.net/2018-04-10-Pour-un-service-public-des-donnees>, aber auch in Le Monde Diplomatique vom 7. Januar 2017.
- ¹⁷⁸ Morozov: <https://blog.mondediplo.net/2016-12-15-Pour-un-populisme-numerique-de-gauche> (i. f.)
- ¹⁷⁹ Sofern man sie überhaupt eindämmen kann, wie sich Cuvelliez fragt
- ¹⁸⁰ Vgl. « Fermeture de BuzzFeed France: quel modèle économique pour les médias en ligne ? » unter https://abonnes.lemonde.fr/actualite-medias/live/2018/06/08/fermeture-de-buzzfeed-france-quel-modele-economique-pour-les-medias-en-ligne_5311624_3236.html.
- ¹⁸¹ Verschiedene Beispiele von gehackten autonomen Fahrzeugen: <https://www.01net.com/actualites/voiture-connectee-voici-les-hacks-les-plus-fous-des-dernieres-annees-1043464.html>
- ¹⁸² «20 minutes» vom 21.6.18
- ¹⁸³ Gallusser/Ringger, S. 23
- ¹⁸⁴ Sofern das ausserhalb der Theorie überhaupt möglich ist, aber das ist nicht Gegenstand dieses Papiers.
- ¹⁸⁵ Wohlmann
- ¹⁸⁶ Alternatives Economiques, Nr. 379, April 2018, S. 43f.
- ¹⁸⁷ http://europa.eu/rapid/press-release_IP-18-4581_fr.htm
- ¹⁸⁸ Alternatives Economiques, Nr. 379, April 2018, S. 43f.

¹⁸⁹ Thomas Metzinger in <https://www.watson.ch/!586642134>

¹⁹⁰ Vgl. die parlamentarische Initiative 18.420 (Glättli) zum E-Voting.

¹⁹¹ Man muss die digitale Identität im weiteren Sinn = alle Daten, die man produziert, unterscheiden von der digitalen Identität im engeren Sinn = Gesamtheit der Daten, die es ermöglichen, die Identität nachzuweisen, vgl. Jaccard, Ch. 1.2. Nicht zu verwechseln mit der elektronischen Unterschrift, vgl. Jaccard, Rz 48ff.

¹⁹² Jaccard, Rz 23

¹⁹³ Jaccard, Rz 21

¹⁹⁴ Jaccard, Rz 32, 35 und 102

¹⁹⁵ Vgl. die parlamentarische Initiative 18.407 (Reynard)

¹⁹⁶ Entscheidung des Verfassungsrats 2009-580 DC vom 10. Juni 2009.

¹⁹⁷ <http://www.rts.ch/info/suisse/9712679-defaillante-discriminante-l-application-d-indemnisiation-des-cff-critiquee.html>

¹⁹⁸ https://abonnes.lemonde.fr/economie-mondiale/article/2018/06/24/internet-la-bataille-du-cable-ne-fait-que-commencer_5320491_1656941.html . Google besitzt z.B. bereits 4 Unterwasserkabel, und bis 2019 werden es 7 sein. Die GAFA sind in 22 Konsortien vertreten, die solche Kabel betreiben.

¹⁹⁹ Gemäss Definition der WTO: <http://www.ilo.org/global/topics/decent-work/lang--fr/index.htm>

²⁰⁰ Maas, Art. 7

²⁰¹ Dazu könnte die Übernahme einer Verantwortlichkeit in Form von «Risiko-Management» führen, vgl.

Lohmann.

²⁰² Degryse, S. 47

²⁰³ Vgl. zu diesem Thema mit vielen Details und Beispielen Schwaab