

Digitalisierung und Menschenrechte

Chancen und Bedrohungen

Vorwort

Befeuer durch massive Investitionen hat sich die Innovation der Informationstechnologie in den letzten Jahren so stark beschleunigt, dass unsere gesellschaftliche und politische Entwicklung mit dem technologischen Fortschritt nicht mehr Schritt hält. Viele Menschen fühlen sich heute von der Digitalisierung bedroht. Sie stellen die Frage, welche ihrer Menschenrechte dadurch gefährdet sind und wie die Regierungen sie schützen werden.

Wir identifizieren fünf relevante Bausteine der aktuellen Digitalisierung und untersuchen, welche Artikel der erstmals 1948 von der UNO definierten [Allgemeinen Erklärung der Menschenrechte](#) in welcher Form betroffen sein könnten.

Ich selber war als einer der ersten Absolventen des Informatikstudiums an der Technischen Universität Wien anfangs begeistert von den vielen Chancen, die die Digitalisierung für die Weiterentwicklung unserer Gesellschaft versprach. Verantwortlich für Datenverarbeitung und Logistik organisierte ich für einen großen Einzelhandelskonzern die Umstellung auf damals zeitgemäße Computertechnik. Dann implementierte ich als [selbständiger Unternehmensberater](#) viele [IT-Projekte](#) für die Privatwirtschaft und die öffentliche Verwaltung. Schließlich organisierte ich den [Ausbau des Internets](#) in Österreich als [Vorstand der Internet Stiftung Austria](#). Für die Unternehmerseite brachte die Digitalisierung viele Vorteile: Automatisierung, Optimierung und vor allem Kostenreduktion. Doch im Laufe der Zeit machen sich auch negative Nebenwirkungen vor allem auf sozialer Ebene bemerkbar: Stress am Arbeitsplatz, Datenmissbrauch, Diskriminierung, Hass-Kampagnen und Fake-News. Heute verdrängt eine zunehmende Skepsis meine anfängliche Euphorie und es ist mir ein Anliegen, die Auswirkungen der Digitalisierung auf unsere Menschenrechte näher zu untersuchen. Damit wir die Brisanz der möglichen Chancen und Bedrohungen objektiver einschätzen können, ist ein Überblick über die Bausteine und die Entwicklungsgeschichte der Digitalisierung hilfreich.

Geschichte der Informationstechnologien

Ein kurzer Blick auf die bisher von Menschen entwickelten Informationstechnologien zeigt uns, dass jede neue Entwicklungsstufe von einschneidenden gesellschaftlichen Veränderungen begleitet war. Historisch erkennen wir sechs disruptive Innovationen:

1. **Sprache:** ca. 100.000 v. Chr. (überlebensnotwendige Kommunikation und Kooperation, Weitergabe von Wissen, Geschichten, Mythen, Gerüchte)
2. **Schrift:** ab ca. 3200 v. Chr. (Heilige Schriften, Buchführung, Gesetze)
3. **Buchdruck:** 1450 n. Chr. (Massenproduktion, Verbreitung von Wissen)
4. **Zeitungen:** ab 1650 (Massenverbreitung von Nachrichten)
5. **Telekommunikation:** ab 1837 (Telegraf, Telefon, Radio, Fernsehen)
6. **Computer, Digitalisierung:** ab 1940 (Turing, Rechner, PC, Smartphone, Internet)

Bei jeder neuen Entwicklungsstufe folgten auf anfängliche Begeisterung Ernüchterung durch negative soziale Auswirkungen und auch Missbrauch (z.B.: falsche Gerüchte, gefälschte Bibelversionen, Hexenliteratur, Sensationsjournalismus, Manipulation, Trend zu „Bad News“). Bisher gelang es uns, technologischen Wildwuchs durch Regulierung und diverse Korrekturmechanismen (z.B.: autonome Aufsicht, Beiräte, Redundanz, Zensur, Zeugenschaft) einzudämmen und negative Entwicklungen zu reduzieren. Aus heutiger Sicht macht uns das in der aktuellen Phase der Digitalisierung große Schwierigkeiten und wir ringen um notwendige regulatorische Vorgaben.

Als Ursache vermuten wir, dass die Digitalisierung einen weitaus massiveren Einfluss auf unsere Wahrnehmung der Realität ausübt als bisher: im Computer wird ein digitales Abbild der Wirklichkeit simuliert und manipuliert. Ziel ist meist eine Optimierung der realen Welt. Oft geht es um Gewinnsteigerung von Unternehmen und die Hoffnung, in komplexen Aufgabenstellungen mit digitaler Unterstützung bessere Entscheidungen zu treffen.

Die digitale Simulation der Realität durch Computer hat heute einen hohen Grad an Perfektion erreicht. Zum besseren Verständnis erinnern wir uns an das [Höhlengleichnis von Platon](#):



Plato's Cave, Quelle: https://www.reddit.com/r/underthesilverlake/comments/foa7rc/platos_allegory_of_the_cave/

Menschen sitzen in einer Höhle gefesselt vor einer Wand, auf die Schatten von Gegenständen projiziert werden (heute kann es auch ein Bildschirm sein). Diese Objekte werden von Wächtern an einem Feuer vorbeigetragen. Die Menschen haben nie etwas anderes gesehen und glauben, dass diese Schatten die ultimative Realität sind.

Informationstechnologie erzeugt stets ein **reduziertes Abbild** der Realität und dieses Abbild kann - absichtlich oder unbeabsichtigt – Fehler enthalten. Die Digitalisierung

simuliert die Realität heute nahezu perfekt. Das digitale Abbild erscheint schöner, hypnotisiert und verführt uns, darin zu verweilen. Die mögliche Folge ist zunehmender Realitätsverlust.

Computer und Digitalisierung

Die Grundidee zur 6. Informationstechnologie, dem digitalen Computer, formulierten [Charles Babbage](#) und [Ada Lovelace](#) 1837 mit ihrem Konzept der [Analytical Engine](#). Zur Zeit des 2. Weltkriegs entwickelten [Alan Turing](#) und [Kurt Gödel](#) die mathematischen Theorien dazu. [Konrad Zuse](#) gelang 1941 im Nazi-Deutschland die erste Realisierung mit dem Digitalrechner [Z3](#). 1956 begann die Ära der kommerziellen [Großrechner](#) mit dem Aufstieg der Firmen IBM, Univac und Siemens. 1976 kamen die ersten [Personal-Computer](#) von Apple und IBM auf den Markt.

Beschleunigt durch große Investitionen und wissenschaftliche Innovationen entwickelten sich dann viele Teilbereiche der Informatik. Komplexe Aufgabenstellungen wurden nach dem Prinzip „[Teile und Herrsche](#)“ in logisch getrennte Funktionen modular aufgeteilt.

Wir betrachten fünf wichtige Bausteine der Digitalisierung mit ihren Funktionen und analysieren ihre positiven und negativen Auswirkungen auf die Menschenrechte und unsere Gesellschaft:

1. [Internet](#) und [WWW](#)
2. [Big Data](#)
3. [Smartphone](#)
4. [Soziale Netzwerke](#)
5. [Künstliche Intelligenz](#)

Diese Bausteine wurden von vielen Wissenschaftlern weltweit in egalitärer Zusammenarbeit entwickelt. Viele Standards und Architekturprinzipien wurden in vorbildlich demokratischen Verfahren ausgehandelt und abgestimmt, ohne von staatlichen Organisationen durch gesetzliche Normen behindert zu werden. Leider erleichtert dieser regulatorische Freiraum heute einigen machtbesessenen Techno-Oligarchen diese Technologien zu monopolisieren und zum Nachteil unserer Gesellschaft ohne Rücksicht auf die Menschenrechte auszubeuten.

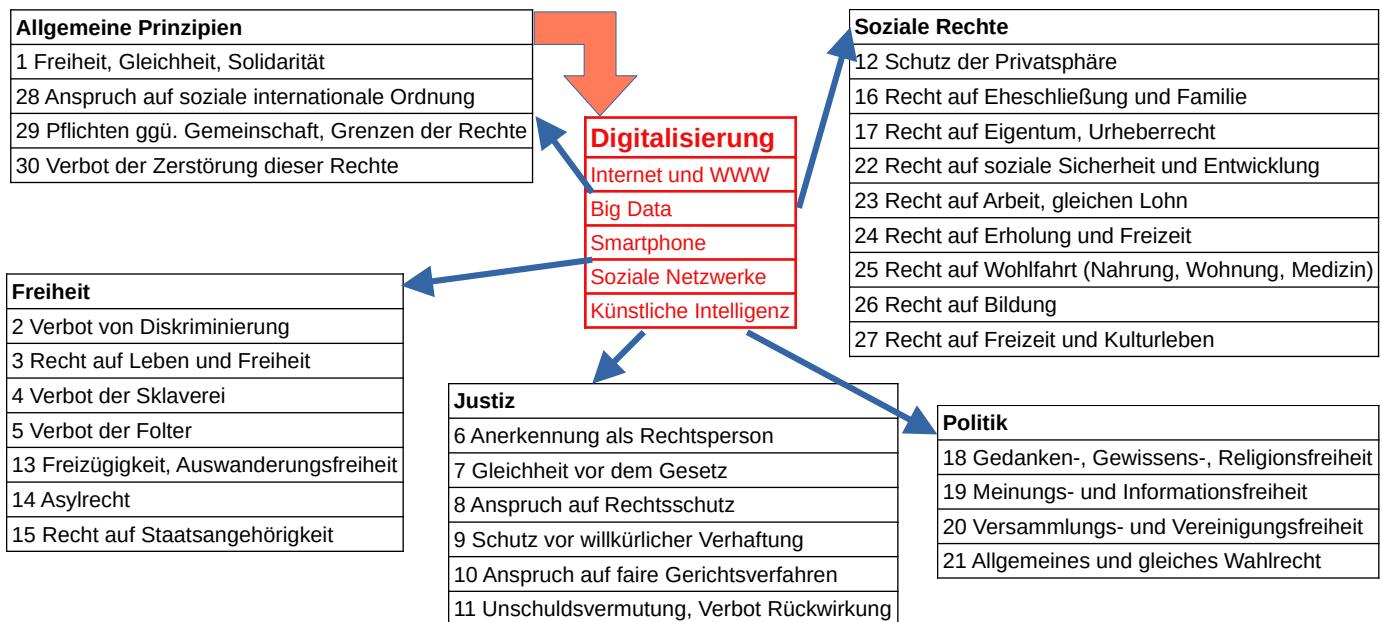
Völlig missachtet werden dabei Art. 1 der Allgemeinen Erklärung der Menschenrechte: „**Alle Menschen sind frei und gleich an Würde und Rechten geboren. Sie sind mit Vernunft und Gewissen begabt und sollen einander im Geist der Solidarität begegnen.**“ und Art. 29.1: „**Jeder Mensch hat Pflichten gegenüber der Gemeinschaft, in der allein die freie und volle Entfaltung der eigenen Persönlichkeit möglich ist.**“

Wir müssen uns mit Nachdruck dafür einsetzen, dass die Balance zwischen Rechten und Pflichten bei der weiteren Entwicklung der Digitalisierung wieder hergestellt wird.

Übersicht Menschenrechte versus IT-Bausteine

Die fünf relevanten IT-Bausteine *Internet und WWW, Big Data, Smartphone, Soziale Netzwerke* und *Künstliche Intelligenz* wirken sich positiv und negativ auf die Menschenrechte aus (blaue dünne Pfeile in der Abbildung unten). Diese fassen wir zur besseren Übersicht logisch zu den fünf Gruppen *Allgemeine Prinzipien, Justiz, Freiheit, Soziale Rechte* und *Politik* zusammen.

Von unseren demokratisch gewählten Regierungen dürfen wir erwarten, dass sie die fünf IT-Bausteine ausreichend regulieren (roter dicker Pfeil), wie es von den Menschenrechten in der Gruppe *Allgemein* gefordert wird, damit sie alle Menschenrechte möglichst positiv fördern und möglichst wenig verletzen.



Wechselwirkungen zwischen Menschenrechten und Digitalisierung

1. Internet und WWW

1969 entwickelte die US-Army das [ArpaNet](#): Durch einen gegnerischen Atombombenschlag sollte nicht das gesamte Verteidigungssystem lahmgelegt werden. Nach dem Prinzip „*no single point of failure*“ wurde von Wissenschaftlern ein redundantes Netzwerk von autonomen Rechnern ohne übergeordnete Zentrale aufgebaut – eine egalitäre Architektur, die durchaus im Konflikt mit den hierarchischen Strukturen der Militärs stand. Rasch wurde das dann [Internet](#) genannte Netzwerk von der Wissenschaft und später auch von der Wirtschaft zur effizienten Kommunikation genutzt.

Einen starken Schub an Benutzerfreundlichkeit bewirkte [Tim Berners-Lee](#) 1989 am [CERN](#) mit dem Konzept der *Hypertext Markup Language* [HTML](#) auf der Basis des dann weltweit standardisierten [HTTP-Protokolls](#). Mit einem Schlag waren dadurch viele Menschen in der Lage, Informationen aus dem Internet einfach und gratis zu beziehen und miteinander zu kommunizieren. Die positive Wirkung auf die Entwicklung der menschlichen Gesellschaft und die Stärkung der Menschenrechte und Demokratisierung wurden euphorisch gefeiert. Bis 2000 wurde das Internet und Informationstechnologie noch weitgehend in staatlichen Universitäten weiter entwickelt.

Leider endete diese Phase der egalitären und selbstorganisierten Innovation. Zahlreiche [Spin-Offs](#), Privatisierungen und Unternehmensgründungen entstanden in rechtlichen Freiräumen. Ab 2010 konnten (und wollten?) staatliche Instanzen die schleichende Aneignung und Vermarktung durch digitale Großkonzerne wie Google, Amazon, Apple, Microsoft, Facebook, Twitter, usw. nicht mehr aufhalten. Heute wird das Internet weitgehend von Techno-Oligarchien ausgebeutet. Die Bequemlichkeit der Nutzer:innen wird dazu verwendet, Daten über ihr Verhalten wild zu sammeln und ihre Entscheidungen (z.B.: Konsum, Politik oder Lebensführung) zu steuern.

Anschaulich mit vielen Beispielen beschreiben [Shoshana Zuboff](#) in ihrem Buch „Surveillance Capitalism“ und [Janis Varoufakis](#) in „Technofeudalism“ diese bedauerliche Entwicklung. Gemäß der „Großen Transformation“ von [Karl Polanyi](#) (1886-1964) werden nach Land, Arbeit und Geld nunmehr auch unsere persönlichen Daten und unser Verhalten als Marktobjekt verkauft und ausgebeutet.

Es entstanden ungeheure virtuelle Reichtümer an Börsenwerten:

Rank	Name	Industry	Marketcap	Country
1	NVIDIA	Chip manufacturer GPU & AI	\$4.566.036.250.624,00	United States
2	Apple	Consumer electronics	\$4.052.613.332.992,00	United States
3	Alphabet (Google)	Semiconductor manufacturing	\$3.797.195.161.600,00	United States
4	Microsoft	Internet services & advertising	\$3.623.520.043.008,00	United States
5	Amazon	E-commerce, cloud computing	\$2.485.795.946.496,00	United States
6	Meta Platforms (Facebook)	Social media & digital advertising	\$1.678.545.387.520,00	United States
7	Broadcom	Semiconductor manufacturing	\$1.658.734.641.152,00	United States
8	TSMC	Semiconductor manufacturing	\$1.553.772.969.984,00	Taiwan
9	Saudi Aramco	Oil & gas production	\$1.523.966.332.076,00	Saudi Arabia
10	Tesla	Electric vehicles	\$1.511.351.910.400,00	United States
Per 2025-12-31			Source: https://companiesmarketcap.com/	

Neun von den zehn Firmen mit der größten Marktkapitalisierung erzielen ihre Gewinne mit Digitaltechnologie; [Nvidia](#) hat als Hersteller von Grafik-Chips aktuell einen Börsenwert von mehr als 4,5 Billionen USD (englisch „Marketcap“ > 4.500.000.000.000,-).

Wie wirkt sich das Internet auf die Menschenrechte aus? Besonders positiv waren anfangs die Auswirkungen auf Art. 1 [Freiheit, Gleichheit], Art. 18 [Gedanken-, Gewissens-, Religionsfreiheit], Art. 19 [Meinungs- und Informationsfreiheit], Art. 24 [Recht auf Erholung und Freizeit] und Art. 26 [Recht auf Bildung]. Die zunehmende Kommerzialisierung und die professionelle Nutzung durch autoritäre Organisationen führt aber jetzt zu gravierenden Einschränkungen bei Art. 2 [Verbot von Diskriminierung] durch Hetzpropaganda, Art. 4 [Verbot der Sklaverei] mit vielen dokumentierten Beispielen von Menschenhandel, Zwang zu Prostitution und Kinderpornografie im DarkNet, Art. 11 [Unschuldsvermutung] durch gewissenlosen Journalismus, Art. 18 [Gedanken-, Gewissens-, Religionsfreiheit] durch Verhetzung, Art. 19 [Meinungs- und Informationsfreiheit] und Art. 20 [Versammlungs- und Vereinigungsfreiheit]. Seit im [DarkNet](#) sogar Morde anonym bestellt und via Kryptowährung bezahlt werden können, erleidet der Staat gravierende Kontrollverluste durch trickreiche Nutzung der Internettechnologie; siehe: <https://hitmanscam.org/>

Aber auch Privatpersonen können die Kontrolle über ihr Eigentum verlieren. Die erstmals von [Günther Anders](#) angesproche **Auflösung des Eigentums** wird am Beispiel von Updates von Gebrauchsgegenständen über das Internet klar erkennbar, wenn erworbene Artikel plötzlich wesentliche Eigenschaften ändern oder sogar verlieren:

- Nach der Insolvenz des E-Auto Herstellers [Fisker](#) wurden etliche dieser Autos [unbrauchbar](#), weil sie ohne Kontakt zum dann abgeschalteten Server nicht mehr starten konnten.
- Einfache Saugroboter des [Vorwerk Konzerns](#) wurden durch willkürliche Einstellung der notwendigen US-Cloudservices unbrauchbar. Konsumenten sollten sich diese Gefahr der plötzlichen Wertminderung beim Kauf von Geräten bewusst machen.
- Für einfache Nutzer:innen kaum zu verhindernde Firmware-Updates über das Internet verändern den Leistungsumfang vieler elektronischer Geräte über Nacht (u.a.: Smartphones, Wärmepumpen, Stereoanlagen, Fernseher)

So wird jedenfalls Art. 17 [Recht auf Eigentum] deutlich verletzt.

2. Big Data

Bei vielen kommerziellen IT-Anwendungen (z.B.: [SAP](#), [Oracle](#)), aber auch in der Wissenschaft sind große Datenmengen zu verwalten. Diese Aufgabe wurde ab 1970 durch [Relationale Datenbanksysteme](#) theoretisch aufbereitet und praktisch durch leistungsfähige Systeme zur Speicherung und Suche realisiert. Daten werden dabei in Tabellen organisiert, jedem Datenobjekt entspricht eine Zeile und die einzelnen Eigenschaften jedes Datenobjekts werden in Tabellenspalten gespeichert.

2010 gab es einen weiteren Entwicklungsschub: [Big Data](#), [Suchmaschinen](#), [OpenSearch](#) und [invertierte Listen](#) ermöglichen eine massive Leistungssteigerung. Riesige Datenmengen können heute einfach und rasch durchsucht und verknüpft werden. Das ist sehr förderlich für viele Menschenrechte, besonders Art. 1 [Freiheit, Gleichheit], Art. 19 [Meinungs- und Informationsfreiheit] und Art. 26 [Recht auf Bildung]. Andererseits gefährdet der effiziente Zugriff und vor allem das Verknüpfen unabhängiger Datenbestände mehrere Menschenrechte, besonders Art. 2 [Verbot von Diskriminierung], Art. 7 [Gleichheit vor dem Gesetz], Art. 9 [Schutz vor willkürlicher Verhaftung], Art. 11 [Unschuldsvermutung], Art. 12 [Freiheitssphäre des Einzelnen], Art. 18 [Gedanken-, Gewissens-, Religionsfreiheit], Art. 19 [Meinungs- und Informationsfreiheit] und Art. 20 [Versammlungs- und Vereinigungsfreiheit].

Die **unrechtmäßige Verknüpfung** getrennter Datenbestände ermöglicht [Profiling](#) durch Schnittmengenbildung über gemeinsame Identifikationsmerkmale (Kreditkartennummer, Telefonnummer, SVNR, Passnummer, E-Mail-Adresse) und zeitliche und räumliche Koinzidenz. Damit kann dann auch aus anonymisierten Einzeldaten auf das Individuum zurückgeschlossen werden. Vorhersage und Beeinflussung persönlichen Verhaltens werden so möglich; automatisiert und verstärkt durch Algorithmen des maschinellen Lernens.

Zur Illustration zeichnen wir ein **düsteres Zukunftsbild**: In 5 Jahren übernimmt ein autoritäres rechtsradikales Regime in einem Staat (eventuell sogar in Österreich) die Regierungsgeschäfte. Der neue Innenminister möchte hart durchgreifen und linksliberale Personen identifizieren, isolieren und als potenzielle Terroristen verhaften lassen. Dazu wird eine Gruppe von Informatiker:innen beauftragt, alle relevanten Datenbestände nach kompromittierenden Fakten zu durchsuchen und zu verknüpfen. Für jede Person werden Terrorpunkte durch die Summe irgendwelcher verdächtiger Eigenschaften errechnet und alle Personen über einem bestimmten Schwellwert werden zuerst genau überwacht und später verhaftet. Dazu werden folgende Daten durchsucht: Melderegister, Arbeitsamt, Finanzdaten, Passamt, Strafregister, Tickets, Zahlungsdaten von Kreditkarten und Bankomaten, Gesundheitsdaten, Bewerbungen, Bondaten des Einzelhandels usw. So könnte eine Überweisung aus Persien beispielsweise 120 Terrorpunkte ergeben, 3-mal Wechseln der Meldeadresse 30, Bart am Passfoto 50, Besuch einer Moschee 20, Einkauf von Falafel 5, von Schweinefleisch aber -20, usw... Sie finden das übertrieben? In den USA ist das bereits Realität; siehe [Homeland Security](#) und: „[The Trump administration is building a national citizenship data system](#)“.

Im Dezember 2025 beschloss der [Europäische Rat](#), mit den USA über eine [Enhanced Border Security Partnership \(EBSP\)](#) zu verhandeln, die US-Behörden den [automatisierten Zugriff](#) auf polizeiliche und biometrische Daten von EU-Bürger:innen einräumen wird.

Interessant ist der Umstand, dass wir in Österreich mit dem vorbildlichen [Datenschutzgesetz aus 2000](#) strenge und klare Bestimmungen gegen den Missbrauch personenbezogener Daten hatten. Beispielsweise forderten damals die §§ 6, 7 und 9 DSG2000, dass Daten nur zu vorher klar definierten Zwecken und mit den zur Erreichung dieser Zwecke „gelindesten“ Mitteln verarbeitet und weitergeleitet (meint auch: verknüpft) werden dürfen und dabei der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat. Leider wurde das durch die Adaption an die [Datenschutzgrundverordnung](#) der EU 2016 zu Gunsten von Unternehmen und Behörden verwässert. Allerdings wurden auch die Auskunftsrechte der Betroffenen konkretisiert.

Besonders beunruhigend sind die Strategien mancher US-IT-Konzerne, Daten über österreichische Schulkinder zu sammeln: Das österreichische Bildungsministerium [BMB](#) vergrößert mit seiner Geräteinitiative [Digitales Lernen](#) die Abhängigkeit von Microsoft, indem es veraltete und überteuerte Tablets mit proprietärer Software für die Schüler ab der 5.Schulstufe vorschreibt. Diese Geräte sind noch dazu mit [unzureichendem Schutz](#) gegen schädliche Inhalte ausgestattet. Die österreichische Datenschutzbehörde (DSB) hat dazu entschieden, dass [Microsoft 365](#) Education gegen die DSGVO verstößt, indem es Schüler ohne ausreichende Einwilligung trackt und Auskunftserteilungen ignoriert.

<https://noyb.eu/de/noyb-win-microsoft-365-education-tracks-school-children>

<https://medienbildung.at/aktuelles/datenschutz-entscheidung-in-sterreich-microsoft-365-education-verstoss-gegen-dsgvo/>

Die [Entscheidung](#) der österreichischen [DSB](#) zeigt exemplarisch, wie tief das Problem reicht: Es geht nicht um einzelne fehlerhafte Einstellungen oder unklare Formulierungen, sondern um ein Geschäftsmodell, das auf systematischer Intransparenz basiert. Microsoft gestaltet seine Produkte so, dass Schulen auf eine [Blackbox](#) vertrauen müssen, ohne nachvollziehen zu können, welche Daten erhoben, wohin sie übertragen und wofür sie letztlich verwendet werden. Die Schulen tragen formal die Verantwortung, während die tatsächliche Macht über Daten und Technik vollständig beim Konzern bleibt.

<https://www.kuketz-blog.de/kommentar-microsoft-365-education-auch-in-deutschland-will-microsoft-nicht-verantwortlich-sein/>

3. Smartphone

Aus den ersten [Mobiltelefonen](#) basierend auf digitaler Funktelefonie entwickelten sich bald kleine leistungsfähige Computer ausgestattet mit Mikrofon und Lautsprecher, Kamera und Bildschirm mit diversen Sensoren ([GPS](#), Kompass, Beschleunigung, Temperatur, usw.) in den zwei Produktgruppen [Android](#) und [iPhone](#). Heute sind weltweit etwa 7 Mrd. Smartphones täglich in Gebrauch; in Österreich sind ca. 22 Mio. [SIM-Karten](#) im Umlauf. Sie werden wegen ihrer bequemen Verwendung geradezu euphorisch verwendet; die ständige Erreichbarkeit, die vielfältigen Kommunikationsmöglichkeiten und die Verfügbarkeit diverser Informationsquellen fördern die ständige Benutzung.

Mittlerweile hat sich das [Smartphone](#) auch zum idealen Überwachungsgerät entwickelt. Viele einfach zu installierende Apps sammeln laufend Daten über gesendete und empfangene Nachrichten. Informationssuchen, Standorte, ja sogar die Anzahl der Schritte und Herzschläge können aufgezeichnet werden und von unkontrollierbaren internationalen Rechenzentren in der [Cloud](#) gespeichert und verarbeitet werden (siehe auch Abschnitt Big Data). Bei den Nutzer:innen wird die Angst gefördert, etwas zu versäumen ([FOMO](#), *fear of missing out*) und zwingt sie zu ständigem Online-Sein.

Die [Aufmerksamkeitsspanne](#) der Menschen wird immer kürzer (von 13 Sekunden im Jahr 2000 auf heute 8 Sekunden) und die analoge zwischenmenschliche Kommunikation wird zunehmend verlernt. Realitätsflucht und Vereinsamung nehmen bedrohlich zu. Die Weltgesundheitsorganisation [WHO](#) hat dieses Krankheitsbild in der [International Classification of Diseases](#) unter 6C51.0 dokumentiert; siehe auch: <https://www.netdoktor.at/krankheiten/internetsucht/>

Wie wirkt sich die massive Verbreitung des Smartphones auf die Menschenrechte aus? Da es ständig verfügbar ist, können Menschenrechtsverletzungen und behördliche Übergriffe einfach dokumentiert werden (Art. 2-9). Bürger:innen können einfach recherchieren, welche Rechte ihnen zustehen (Art. 10-27). Negativ wird das Smartphone von radikalen Gruppen effizient als Werkzeug zur Verhetzung und Verbreitung von Fake-News genutzt (Art. 1, 2, 18, 19). Bewegungs- und Kommunikationsprofile können damit einfach erstellt werden (Art. 9, 11-14) und erleichtern so den Daten-Missbrauch von Behörden, der Privatwirtschaft und Kriminellen.

4. Soziale Netzwerke

Eine treffendere Bezeichnung wäre: „*digitale Kommunikationsplattformen*“ Ursprung war das *Short Message Service SMS* der Mobilfunkindustrie. Die asynchrone Kommunikation und ständige Erreichbarkeit wurde vor allem von Studenten und Technikern als vorteilhaft empfunden. Als erste erfolgreiche Plattformen entstanden [Facebook](#) und [Twitter](#) (jetzt „X“), anfangs durchaus mit dem Ziel der Förderung sozialer Kommunikation, später als enorm effiziente Marketing-Maschinen und ertragreiche Geldquellen. Heute wird erbittert um Marktanteile gekämpft, ständig entstehen neue Kopien; u.a.: [Bluesky](#), [Instagram](#), [TikTok](#), [WhatsApp](#), [Reddit](#), [Signal](#), usw.

Zur Ertragssteigerung werden hochkomplexe Algorithmen verstärkt durch maschinelles Lernen eingesetzt, die das sogenannte „[User Engagement](#)“ maximieren sollen und mit optimiertem „[Addictive Design](#)“ eine Art von Suchtverhalten bei den Nutzer:innen erzeugen, um sie möglichst lange und häufig zu binden. Mit psychologischen Tricks wie variable Belohnungen, Likes oder Ranking werden Gewohnheiten geschaffen, die zu übermäßigem Konsum führen.

Nach [Daniel Kahneman](#) (*Thinking, Fast and Slow*) reagieren Menschen in zwei Varianten auf Information:

- **schnell** und reflexartig auf anscheinend bedrohliche Ereignisse und
- **überlegt**, wenn sie glauben, mehr Zeit investieren zu können

Die Algorithmen der digitalen Kommunikationsplattformen priorisieren daher alarmierende Nachrichten mit dem Ziel, rasche emotionale Reaktionen ohne kritische Reflexion hervorzurufen. Derart manipulierte Inhalte werden nahezu unbewusst akzeptiert und als relevante Erfahrung verinnerlicht. Diese Mechanismen werden deutlicher erkennbar, wenn wir uns die Unterschiede der [Kommunikationsformen](#) vergegenwärtigen:

Analoge Kommunikation, das persönliche Gespräch, ist charakterisiert durch:

- Viele Sinne sind einbezogen (Tonfall, Mienenspiel), kontextreich
- Beteiligt sind meist sozial nahe, vertraute reale Personen
- [Reputationsmanagement](#) und Legitimation sind selten erforderlich
- Sofortiges Feedback ist in vielen Formen möglich
- Keine schriftliche Dokumentation, Korrektur / Entschuldigung einfach
- Die [Reichweite](#) ist lokal beschränkt
- Menschen bestimmen den Grad an Vertraulichkeit selbst

Digitale Kommunikation (*posts, messages*) ist eingeschränkt durch:

- Kontextarmut, nur Schrift und Bild
- Angst vor Missverständnissen zwingt zu expliziten schärferen Nuancen
- Teilnehmer:innen sind sozial entfernt, halb anonymes Personenbild
- Expliziter Wettbewerb (Ranking über #follower, #likes, #posts, ...)
- Damit wird zu intensivem Reputationsmanagement motiviert
- Feedback ist zeitlich entkoppelt, keine sofortige Reaktion möglich
- Permanente Dokumentation, Korrektur / Entschuldigung schwierig
- Die Reichweite ist potenziell unendlich
- Vertraulichkeitsgrad fremdbestimmt; Algorithmen bestimmen, wer was sieht

Die digitale Ansprache ohne analoge Begleitinformationen wie Körpersprache, Augenkontakt, Mienenspiel, Stimmlage und ohne sofortige Feedback-Möglichkeit sperren ihre Benutzer in wirksame [Echokammern](#). Korrigierende alternative Informationen werden ausgefiltert. Meinungen und Haltungen werden verfestigt und radikalisiert. Der so erzeugte Realitätsverlust schafft Raum für wirksame Manipulation. Logisches Denken wird absichtlich ausgeschaltet und abtrainiert.

In den Medien häufen sich vereinfachende Nachrichten über die Radikalisierung über soziale Netzwerke: „*Der Terrorist hat sich über TikTok radikalisiert*“. In Wirklichkeit handelt es sich um einen komplexen, mehrstufigen Prozess:

- Es beginnt meist harmlos über allgemeine Themen wie:
Armut, Hunger, Wohnungsnot, Ungleichheit, Enttäuschung, Neid
(„Migranten kriegen mehr als wir“)
- Die Spaltungstendenz ist gut verdeckt („Wir vs. die Anderen“)
- Es folgt positives Feedback, Wertschätzung, Fragen zur Abhilfe
- Verwickeln in Dialoge, Suche nach Ansatzpunkten
- [NLP](#)-Methoden werden professionell eingesetzt
- Übersiedeln in kleinere nicht moderierte Gruppen (u.a. [Telegram](#))
- Zunehmend klare und extreme Aussagen, positives Feedback
- Verleihen von Würde und Sinn
- Übergang in private Kanäle als Belohnung
- Individuelle Ansprache, kleine Aufgaben, Mutproben
- Aufforderung zum Anschlag

Mögliche Gegenstrategien sind: externe Kontrolle, verbesserte Trainingsdaten für Moderation und Löschung, Sensibilisierung und Bildung der Nutzer, Steigerung der Medienkompetenz. Verbieten und Schließen nützt nichts, da Ersatzsysteme rasch aufgebaut werden. Auffallend ist, dass gerade rechtsradikale Organisationen die sozialen Netzwerke sehr professionell und wirkungsvoll nutzen; demokratische Bewegungen agieren derzeit vergleichsweise eher hilflos.

Mittlerweile sind viele bedrohliche Auswirkungen digitaler Kommunikationsplattformen auf die Menschenrechte (Art. 2, 12, 18-22) dokumentiert, u.a.:

- [Massaker an den Rohingya](#) in Myanmar 2017 durch Verhetzung auf Facebook maßgeblich mitverursacht
- [Wahlsieg von Bolsonaro](#) in Brasilien 2018 durch Verhetzung und Fake News auf Twitter und YouTube
- [Selbstmord von Dr. Kellermayr](#) in Oberösterreich mitverursacht durch Corona Hasskampagnen auf Twitter und Facebook
- Der [Sturm aufs Capitol 2021](#) und die Kampagnen von [Qanon](#) wurde großteils über digitale Kommunikationsplattformen organisiert.

Natürlich kann der positive Nutzen digitaler Kommunikationsplattformen für die Menschenrechte (Art. 1, 2, 18-27, 28, 29) nicht geleugnet werden; viele Menschenrechtsbewegungen und Aktionen wären ohne sie kaum so machtvoll organisiert worden.

5. Künstliche Intelligenz

Hier bevorzugen wir die klarere Bezeichnung „[Maschinelles Lernen](#)“. Leider erzeugen Marketing und Geschäftemacherei heute viel Verwirrung, die wir durch Klarstellung der relevanten Begriffe überwinden wollen.

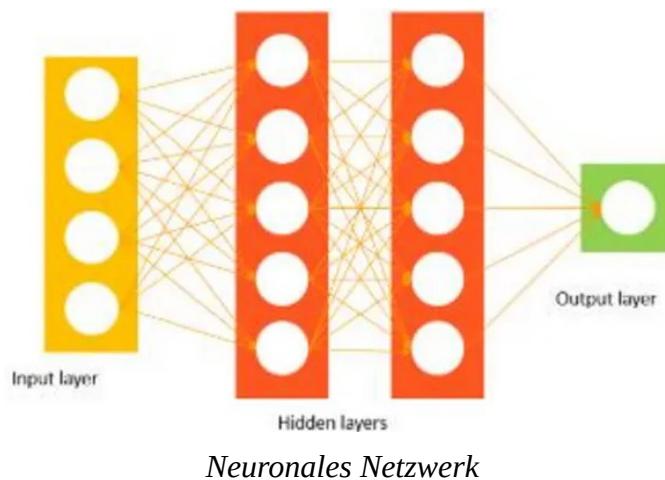
Intelligenz ist die Fähigkeit, selbstständig Ziele über längere Zeit zu verfolgen und dabei aus Erfahrung zu lernen. So kann geeignet programmierte Software Schach spielen, finanzielle Anlagen verwalten oder User Engagement maximieren; sich eben intelligent verhalten. Basierend auf statistischen Wahrscheinlichkeiten trifft sie autonom Entscheidungen und löst komplexe Probleme durch logische Schlussfolgerungen. Wenn die Software bei der Aufgabenstellung auch Mehrdeutigkeiten und unklare Zieldefinitionen akzeptiert, kann das zu nicht vorhersagbaren Resultaten führen.

Traditionell wird Software zur Erfüllung einmal festgelegter Aufgaben mit statischen Programmen entwickelt, die in regelmäßigen Schritten angepasst und verbessert werden (sog. Updates oder Releases). Im aktuellen Hype werden viele längst etablierte Automatisierungsfunktionen als „Künstliche Intelligenz“ vermarktet. Vor zehn Jahren hätte niemand eine simple Heizungsregelung als *intelligent* bezeichnet. Korrekt ist dieser Begriff nur angebracht, wenn sich Computerprogramme zielgerichtet selbst verändern können.

Genau genommen sollten aktuell verwendete Übersetzungsalgorithmen auch nicht als Künstliche Intelligenz verstanden werden. Früher wurde in der Informatik angenommen, dass für eine korrekte Übersetzung ein Verständnis des Textes notwendig ist und es wurden aufwendige Algorithmen zur Analyse und Synthese von Syntax und Semantik entwickelt. Heute werden Millionen von Bücherpaaren in zwei Sprachen digitalisiert und gespeichert. Bei der Übersetzung wird einfach der passendste Textabschnitt in einer Sprache gesucht und der entsprechende Text in der anderen Sprache als Resultat geliefert. Das ist eigentlich Verwendung von Big Data, aber keine künstliche Intelligenz; ein [Plagiat](#) in Perfektion: **geistiges Eigentum wird annektiert** und ausgebeutet.

Bisher generierte die Computerindustrie zwei euphorische Phasen der künstlichen Intelligenz. Die erste begann bereits 1960 mit Versuchen, menschliches Kommunikationsverhalten am Computer zu simulieren. Alan Turing schlug in seinem [Turing-Test](#) ein Setting vor, in dem eine Testperson herausfinden soll, ob sie mit einem menschlichen Partner oder einem simulierenden Computer kommuniziert. Der Informatiker [Joseph Weizenbaum](#) versuchte bereits 1966 mit seinem Programm [Eliza](#) zu demonstrieren, wie mit einem kleinen Computerprogramm menschliches Kommunikationsverhalten vorgetäuscht werden kann. Schließlich endeten diese überzogenen Erwartungen in einer großen Enttäuschung.

Die Grundidee zum maschinellen Lernen wurde bereits um 1960 vom Kybernetiker [Karl Steinbuch](#) in Deutschland mit seiner [Lernmatrix](#) skizziert, aber nicht erfolgreich vermarktet und dann vergessen. Software passt sich dabei während ihrer Verwendung an neue Anforderungen dynamisch an und lernt damit gewissermaßen. Die Struktur simuliert dabei die Funktionsweise des menschlichen Nervensystems. [Neuronale Netzwerke](#) bilden die Erregungsmuster von Eingangsneuronen als *Input* über Schichten von Zwischenneuronen auf die wahrscheinlichsten Ausgangsneuronen als *Output* ab.



Neuronales Netzwerk

Mit Trainingsdaten werden diese Systeme gefüttert, bis sie die gewünschten Resultate mit einer statistisch vorgegebenen Wahrscheinlichkeit liefern. Leider können heute viele dieser Systeme nicht erklären, wie sie zu ihren Resultaten gekommen sind. Das Problem der „[Explainable AI](#)“ ist derzeit Gegenstand intensiver Forschung.

Unleugbar wurden in vielen Bereichen großer Nutzen mit Methoden des maschinellen Lernens erreicht; vor allem in der Medizin (z.B.: Erkennen von Hautkrebs oder Anomalien im Blutbild), der Optimierung industrieller Prozesse (Automobilindustrie), dem Erkennen von Fehlern und Betrug (Kreditkarten) und sogar in der Softwareentwicklung selbst (automatisiertes Erstellen von Computerprogrammen). Dabei handelt es sich im Wesentlichen um das effiziente *Erkennen und Analysieren von Mustern*. Dabei sind uns Computer überlegen, weil sie nicht den **Beschränkungen der menschlichen Informationsverarbeitung** unterliegen.

Bereits [John Locke](#) hat 1660 in seinem „[Seven Phenomenon](#)“ erkannt, dass unser Kurzzeitgedächtnis beim Denken nicht mehr als etwa sieben Dinge („*Chunks*“, Informationsbündel) gleichzeitig berücksichtigen kann und dass diese nach einer kurzen [Aufmerksamkeitsspanne](#) von anderen Informationen verdrängt werden. Dieser Umstand wurde 1956 von [George A. Miller](#) in seiner bedeutenden Arbeit „[The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information](#)“ dokumentiert. Beim maschinellen Lernen können Computer eine potenziell unendliche Menge von Informationen ohne zeitliche Beschränkungen nahezu gleichzeitig verarbeiten. Außerdem können digitale Sensoren eine Vielzahl von Reizqualitäten erkennen, die uns Menschen verborgen bleiben (Ultraschall, Röntgenstrahlen, Funkwellen, ...). Um uns vor einem sog. „[Information Overload](#)“ zu schützen, filtert unser Nervensystem viele vielleicht auch relevante Signale einfach weg, damit wir uns auf wenige, als überlebenswichtig eingestuften Reize konzentrieren können. Digitale Intelligenz ist da leistungsfähiger, sie trifft keine Vorauswahl und hat keine Vorurteile.

Dem gegenüber verursacht die Qualität der Daten, mit denen diese Systeme trainiert werden, derzeit große Probleme. Man spricht hier vom sog. „[Bias](#)“. Darunter versteht man den Umstand, dass die Auswahl und Qualität der Trainingsdaten, aber auch die kommerziellen Interessen und die Haltung aller an der Entwicklung beteiligten Personen die erzielbaren Resultate stark beeinflussen.

So wurden beispielsweise schwarze Frauen von einer von Weißen trainierten KI gar nicht als Menschen erkannt (Art. 2 der Menschenrechte). Der von Microsoft entwickelte KI-Bot [Tay](#) wurde mit Twitter-Messages trainiert und erzeugte dann selbst rassistische und rechtsextreme Posts und musste schließlich abgeschaltet werden.

Seit mehreren Jahren werden sog. *Large Language Models LLM* von Unternehmen, aber auch von Privatpersonen intensiv verwendet. Auch Schüler:innen versuchen damit ihre Aufgaben zu lösen, was viele Lehrpersonen vor neue Probleme stellt. Es handelt sich dabei um KI-Anwendungen, die basierend auf linguistischen Wahrscheinlichkeitsmodellen Texte, Zusammenfassungen, Präsentationen, aber auch Sprache oder Bilder erzeugen. Aus sehr vielen Textdokumenten lernen diese Modelle durch rechenintensives Training und unter immensem Stromverbrauch statistische Wort- und Satzfolge-Beziehungen und liefern dann auf Anforderung die wahrscheinlichste Textfolge als Antwort.

Beispielsweise wird in der Eingabe „*Gib mir ein Rezept für Apfelstrudel*“ erkannt, dass es sich um eine Rezeptanforderung handelt und dann aus vielen eingescannnten Kochbüchern das wahrscheinlichste Rezept als Antwort präsentiert. Natürlich werden dabei Urheberrechte und damit die Menschenrechte auf Eigentum und Arbeit (Art. 17, 23) massiv verletzt.

Systeme wie [ChatGPT](#), [Google Gemini](#), [Microsoft Copilot](#), [Antrophic Claude](#) oder [DeepSeek](#) aus China zeigen bereits eine eindrucksvolle Funktionalität und schreiben selbst funktionsfähige Computerprogramme. Allerdings sind Realitätsbezug und Detailwissen mitunter mangelhaft und es kommt zu [Halluzinationen](#).

Diese Systeme eignen sich Daten aus vielen Quellen an und geben diese in neuer Zusammenstellung als ihre eigenen aus. Oft werden dabei Urheberrechte verletzt (Art. 17) und es häufen sich bereits die Gerichtsverfahren dazu. Handelt es sich hier nicht um ein automatisiertes **Plagiat in Perfektion?** Geistiges Eigentum wird annexiert und als eigene Leistung weiterverkauft.

Nach [Prognosen der OECD](#) werden dadurch viele White-Collar-Jobs vernichtet; Expertenwissen, Berichte schreiben, Überwachung und Kontrolle werden damit kostensparend automatisiert.

Erwähnenswert ist auch der hohe Ressourcenverbrauch beim Lernen der Sprachmodelle. Das Trainieren der Neuronalen Netze [verbraucht enorm viel Strom](#) aus Kraftwerken, deren Errichtung alle Staatsbürger:innen finanziert haben.

Bemerkenswert ist die Häufung von Menschenrechtsverletzungen (Art. 3, 4, 23) beim Training der Sprachmodelle. In Kenia überwachen Arbeiter:innen um einen Hungerlohn unter [unmenschlichen Bedingungen](#) diese Trainingsprozesse.

Das Erzeugen von Information aus alten, eingescannten Daten lässt vermuten, dass dabei nichts wirklich Neues entstehen kann. Ständiges Kombinieren von Altem könnte zu Stillstand und Versteinerung führen. Selbst das chinesische LLM *DeepSeek* meint, dass es selbst keine innovative wissenschaftliche Theorie ähnlich der Thermodynamik entwickeln wird und erinnert an die Grenzen algorithmischer Berechenbarkeit (Turing).

Die durch maschinelles Lernen einfach mögliche Suche, Zusammenfassung und Aufbereitung relevanter Informationen stärken unsere Menschenrechte in vielen Bereichen (Art. 1-3, 6-8, 18, 19, 22-27). Andererseits verletzt ein rücksichtsloser Einsatz zur Gewinnmaximierung die Art. 4, 7, 12, 17 und 30. Künstliche Intelligenz wird auch im Rechtsbereich von Ankläger:innen, Verteidiger:innen und auch Richter:innen eingesetzt, um endlose Aktenberge zu bewältigen. Erst kürzlich musste der Oberste Gerichtshof in Österreich eine von LLMs generierte Nichtigkeitsbeschwerde zurückweisen.

Besonders gravierend sind die Verletzungen der Art. 1-3, 6-11 und 12-15 bei der Suche nach Terroristen. In einigen Bundesstaaten der USA werden Menschen auf Vorschlag der Künstlichen Intelligenz ausgesondert und verhaftet oder es wird ihnen die Einreise verweigert, ohne dass die Software eine nachvollziehbare Begründung liefern kann. Siehe u.a.: Surveillance as a service.

Automatisch erzeugte Fake-News bedrohen unsere Demokratie und damit die Artikel 18-21, 22, 26 und 28. Als schreckliche Horrorvision könnten wir automatisierte Menschenrechtsverletzungen durch autonome Künstliche Intelligenz befürchten, für die sich kein Mensch mehr verantwortlich fühlt.

Langsam scheint auch eine Art **digitaler Mystik** oder Religion aufzukommen.

Digitale Endgeräte und simulierte Realität dienen als neues Opium für das Volk mit dem Versprechen einer Erlösung von allen realen Nöten. Transhumanismus kündet von einer neuen Form von Unsterblichkeit. Evangelisten sagen eine wunderbare Zukunft durch Mind-Uploading und eine harmonische Symbiose mit Künstlicher Intelligenz voraus:

- Ray Kurzweil (Director of Engineering bei Google LLC.) verspricht Unsterblichkeit durch KI: „The Singularity is Nearer. When We Merge with AI (2045)“
- Yi Zeng von der Chinese Academy of Sciences spricht von einer „Sustainable Symbiotic Society of Natural Life and Living AI“
- Elon Musk verkauft über Neuralink sog. Brain-Machine Interfaces und predigt: „Humans will eventually be able to live forever, by uploading their brains into robots“

Falls diese Prophezeiungen doch nicht eintreten, überlegen einige Techno-Oligarchen aber auch einen Plan B: lieber Einfrieren lassen oder ab zum Mars?

Bevor wir uns vor einer hypothetischen Superintelligenz fürchten oder unser Gehirn in sie uploaden wollen, sollten wir ein paar nüchterne Überlegungen anstellen:

Bewusstsein können wir als die Fähigkeit definieren, über sich selbst als handelndes Subjekt zu reflektieren, Handlungen zu bewerten und Gefühle wie Schmerz, Lust, Zufriedenheit, Liebe oder Hass zu empfinden. Diese Fähigkeit könnte man heute mit Simulationen am Computer sicher besser vortäuschen als 1960 beim ersten Hype der Künstlichen Intelligenz. Da sich die Wissenschaften aber offensichtlich noch auf keine klare Definition von Bewusstsein einigen können, sollten wir alle Prophezeiungen, dass Künstliche Intelligenz jemals so etwas wie Bewusstsein entwickeln wird, als reines Marketing bewerten.

Könnte es sein, dass der derzeitige Hype großteils durch beabsichtigte Marktmanipulation ausgelöst wurde und dass Narrative von übermächtigen Intelligenzen eher Rückschlüsse auf die Gier und das übersteigerte Selbstbild der Techno-Oligarchen zulassen? Einige Börsenkurse beginnen jedenfalls gerade zu bröckeln...

Auswirkung auf die Demokratie

Die Voraussetzungen für eine funktionierende Demokratie sind: **Gewaltentrennung**, **Meinungsfreiheit** und ein **Grundverständnis** der diskutierten Inhalte. Daher ist ausreichende Bildung besonders wichtig. Basis ist stets die Kommunikation und damit die Erreichbarkeit aller Bürger:innen. Das war anfangs die Möglichkeit, die Meldungen des Ausrufers zu hören und auf gemeinsamen Plätzen zu diskutieren. Lange dienten möglichst unabhängige Medien wie Zeitungen und Rundfunk der Demokratie. Immer wieder versuchten autoritäre Kräfte, diese Medien zu übernehmen. Diktaturen nutzen Informationstechnologien, um Macht zu gewinnen und zu erhalten, Ordnung zu stabilisieren und ihre Bürger:innen zu kontrollieren. Bis heute gelang es, zum Schutz der Demokratie und der Menschenrechte wirkungsvolle Mechanismen zur Korrektur von Falschinformationen und Fake-News zu installieren.

Heute dient das Internet als meist genutzte Kommunikationsplattform, zunehmend auch über die sozialen Netzwerke. Da diese heute weitgehend von privatwirtschaftlichen Konzernen betrieben werden, steht dort die Maximierung von Gewinnen und die Absicherung erreichter Machtpositionen im Vordergrund. Dieser zunehmende Einfluss bedroht die Menschenrechte und unsere Demokratie. Gerade jetzt reduzieren die Betreiber der Sozialen Netze viele selbst-korrigierende Mechanismen wie Moderation, Selbstkontrolle und externes Auditing.

Damit sich die Staatsbürger:innen objektiv informieren können und gefälschte Informationen, Gerüchte und Verschwörungstheorien erkennen können, ist eine **Steigerung der digitalen Kompetenz** unerlässlich. Diese muss möglichst früh in unserem Bildungssystem einsetzen und uns bis ins hohe Alter begleiten. Derzeit vermissen wir in den Schulen eine solide Computer- und Smartphone-Pädagogik, die meisten Lehrinhalte werden von US-Computerkonzernen wie Microsoft bestimmt. Auch die Beschaffung von Hardware und Software im Bildungsbereich orientiert sich zu stark an den Vorgaben der amerikanischen Computerindustrie.

In den USA kann man die wachsende Gefährdung der Demokratie durch private Internetkonzerne klar beobachten. Immer mehr Aufgaben der staatlichen Sicherheit werden an privatwirtschaftliche Firmen übertragen: So haben bereits 2013 wichtige staatliche Organisationen der US-Regierung ihre Datenverwaltung zumindest teilweise an Palantir Technologies Inc. übertragen; u.a.: CIA, Homeland Security, NSA, FBI, CDC, Marine Corps, Air Force, Special Operations Command und West Point. Dadurch entsteht eine **ungeheure Machtfülle im privaten Bereich**, da alle diese Daten - wie im Abschnitt *Big Data* beschrieben - einfach und unkontrolliert verknüpft werden können. Die dem Ansehen eines demokratischen Staates abträglichen Menschenrechtsverletzungen werden so bequem in privaten Organisationen versteckt. Palantir und ähnliche Unternehmen verdienen dadurch nicht nur enorm viel Geld, sondern häufen eine neue, zukünftig viel wertvollere Kapitalform an: *Daten über uns alle*.

Leider wird die Verantwortung über den Schutz der persönlichen Daten ihrer Bürger:innen auch von vielen europäischen Staaten an amerikanische Datenkonzerne übertragen. So setzen in Deutschland viele Bundesländer Überwachungssoftware von US-Konzernen ein, so zum Beispiel die Polizei Bayern 2024 mit der Software VeRA (Verfahrensübergreifende

Recherche und Analyse). Abgesehen von den entstehenden Menschenrechtsverletzungen wird sich diese Abhängigkeit von den USA angesichts der aktuellen politischen Verhältnisse verhängnisvoll für Europa auswirken. Europa muss hier seine Autonomie rasch zurückgewinnen. Einen gangbaren Weg skizziert das Konzept [EuroStack 2025](#).

Sozialkybernetik: dieser Begriff beschreibt, wie Informationstechnologie schon immer soziale Beziehungen verändert und unsere Gesellschaft einschneidend geformt hat. Laufend werden neue Überwachungsstrukturen und Ordnungssysteme aufgebaut. Fake-News und Angstmacherei gab es schon im Mittelalter; man denke nur an Hexenjagden, Inquisition, Denunziation unter der Herrschaft von Kirche, Dogen, Hitler und Stalin.

Seit 2014 wurde in China ein sogenanntes [Sozialkredit-System](#) aufgebaut, das das Wohlverhalten der Staatsbürger:innen kontrollieren soll:



Quelle: Infographics Group; Text: Bernhard Bartsch, Martin Gottske; Illustration: Christian Eisenberg

Seit der Implementierung der [Schleierüberwachung](#) im Iran ab April 2023 bestrafen Gesichtserkennungsalgorithmen Frauen, die keinen korrekten Schleier in der Öffentlichkeit oder im Auto tragen.

Bewertungssysteme wie [Tripadvisor](#), [docfinder](#), [booking.com](#) werden bei uns intensiv benutzt und erreichen durchaus auch wertvolle Verbesserungen für Konsument:innen.

Wie können wir die Digitalisierung positiver gestalten?

Die Auswirkungen auf unsere Gesellschaft, besonders auf Kinder sind gründlich zu erforschen. Wir brauchen eine bessere und mehr digitale Bildung in den Schulen. Statt simpler Bedienungsanleitungen aktueller Industrieprodukte müssen wir die Grundlagen und Denkmodelle der Informatik lehren und auch das Programmieren üben. Dabei holen wir unsere Kinder aus der Konsumentenrolle und motivieren sie zu aktivem Gestalten.

Eine breite Bildungsinitiative *Digitale Kompetenz und Gesellschaft* sollte alle Altersgruppen einbeziehen.

Wir müssen unsere **Abhängigkeit von US-IT-Unternehmen drastisch reduzieren**. Das gilt genauso für Privatpersonen, Privatunternehmen, aber besonders für den öffentlichen Sektor. Dadurch könnte die Autonomie Europas wesentlich gesteigert werden. Es ist kein Geheimnis, dass viele EU-Staaten noch immer einen Großteil ihrer Daten auf der Basis von Microsoft Produkten verarbeiten und einige ihrer Daten auch auf US-Servern speichern. Als positives Beispiel kündigte die [dänische Regierung](#) im Sommer 2025 die strategische Umstellung von *Microsoft Office* auf das frei verfügbare Open-Source Produkt [LibreOffice](#) an, um ihre digitale Souveränität zu stärken.

Für alle gesellschaftlich relevanten IT-Projekte müsste in Zukunft eine klare, öffentliche Zieldefinition geführt werden, statt stillschweigend unüberlegte Aufträge an privatisierte ehemals staatliche Organisationen zu vergeben; dabei erinnern wir uns beispielsweise an [Kaufhaus Österreich](#) und diverse Tochterfirmen der A1 Telekom Austria AG. Für staatliche IT-Investitionen sollte daher klare Zieldefinition mit einer langfristigen und umfassenden Kosten / Nutzen Bilanz offengelegt werden.

Wir sollten bald über eine Besteuerung der Ernte von **persönlichen und öffentlichen Daten** nachdenken. Vielleicht könnte man auch den Besitz von Daten ins Vermögen einrechnen und überlegen, mittelfristig auch irreführende Werbung und übertriebenes Marketing zu verbieten. Jedenfalls scheint eine laufend angepasste Regulierung der Digitalisierung unerlässlich.

Zusammenfassung

In jeder Phase der Digitalisierung beobachten wir das gleiche zeitliche Muster: Der meist staatlich finanzierte Wissenschaftsbereich entwickelt eine wertvolle Innovation, die anfangs großen Nutzen für die menschliche Gesellschaft verspricht und auch positiv in der Ausübung unserer Menschenrechte verwendet wird. Die egalitäre Zusammenarbeit der Entwickler erfolgt in einem nahezu rechtsfreien Raum. Bis heute sind beispielsweise viele Bereiche im Internet kaum durch gesetzliche Normen geregelt. Dadurch ist es für privatwirtschaftliche Institutionen dann relativ einfach, diese von uns allen finanzierten Innovationen zu übernehmen und zu unserem Nachteil kommerziell auszubeuten. In Beispielen haben wir belegt, dass dabei immer wieder Menschenrechte verletzt werden. Das erleben wir beim Digitalrechner, beim Internet, bei Big Data, dem Smartphone und den sozialen Netzwerken. Heute wird dieser negative Effekt durch den Einsatz Künstlicher Intelligenz vervielfacht.

Digitalisierung wird hauptsächlich zur Gewinnmaximierung auf der Basis von Marketing, Profiling, Diskriminierung und Angstmacherei genutzt. Die dabei entstehenden Verletzungen von Menschenrechten werden in Kauf genommen und kaum verfolgt. Der Nutzen der Digitalisierung verschiebt sich damit eindeutig zur Privatwirtschaft. Das Individuum, der gemeinsame Wohlstand und die menschliche Gesellschaft tragen die Kosten und erleben die Nachteile. Derzeit kommt der Staat seiner Pflicht, die Würde und die Freiheit seiner Bürger, also die Menschenrechte zu schützen, kaum nach. Auf Druck der US-IT Konzerne erwägt so die EU gerade jetzt, Teile ihrer 2024 verabschiedeten KI-Verordnung zu verschieben und zu verwässern.

Ein gutes Beispiel dafür, was alles möglich ist und wie machtlos sich die EU dabei darstellt, ist der [Ausschluss des EU-Richters Nicolas Guillou](#) von beinahe allen digitalen Diensten, weil er Haftbefehle gegen den israelischen Premierminister Benjamin Netanjahu und den ehemaligen Verteidigungsminister Yoav Gallant autorisiert hatte. Die Trump Regierung setzte ihn deshalb im August 2025 auf eine Sanktionsliste und untersagte US-Unternehmen jegliche geschäftliche Interaktion mit ihm. Seitdem funktionieren seine Kreditkarten nicht mehr und der Internetzugang zu Cloudspeichern, Amazon, Airbnb, Expedia und PayPal wurde gesperrt.

Um diese digitalen Bedrohungen zu minimieren und wieder mehr Nutzen für unsere Gesellschaft zu generieren, sollten wir eine Reihe von **Maßnahmen** diskutieren:

- Abhängigkeit von US-IT-Unternehmen drastisch reduzieren
- Auswirkungen auf unsere Gesellschaft, besonders auf Kinder gründlich erforschen
- Bessere und mehr [digitale Bildung in den Schulen](#)
(*Microsoft raus aus unseren Schulen*; siehe 2. Big Data)
- Denkmodelle der Informatik statt Bedienung aktueller Industrieprodukte lehren
- Kinder aus der Konsumentenrolle holen und sie zu aktivem Gestalten motivieren
- Breite Bildungsinitiative Digitale Kompetenz und Gesellschaft
- Klare, öffentliche Zieldefinition für alle gesellschaftlich relevanten IT-Projekte
- Langfristige und umfassende Kosten / Nutzen Bilanz für öffentliche IT-Investitionen
- Besteuerung der Ernte von persönlichen und öffentlichen Daten
- Datenbesitz ins Vermögen einrechnen
- Über ein Eingrenzung und Regulierung von Werbung und Marketing nachdenken
- Laufend angepasste gesetzliche Regelung der Digitalisierung

Im Grunde genommen bilden die Menschenrechte eine wertvolle Leitlinie für die weitere Entwicklung der Informationstechnologie: bei jedem bestehenden oder neu entwickelten Baustein der Digitalisierung müssen wir gewissenhaft prüfen, welche Menschenrechte dadurch gefördert oder verletzt werden, und mit Nachdruck durchsetzen, dass die Bilanz zwischen Schaden und Nutzen für unsere Gesellschaft positiv ausfällt.

Wenn wir weiter untätig zuschauen und den Missbrauch der Informationstechnologie durch Techno-Oligarchen zulassen, müssen wir uns den Vorwurf gefallen lassen, selbst die Menschenrechte zu verletzen. Diktaturen entstanden stets durch voreilige Unterwerfung und Akzeptanz. Wir müssen unsere Zukunft selbst in die Hand nehmen und aufhören, die Internet-Milliardäre zu bewundern und vor ihrem rein virtuellen Reichtum und ihrer vorerst scheinbaren Macht zu kapitulieren. Noch können wir die Schwachpunkte in ihren Strategien identifizieren und diese zum Widerstand erfolgreich nutzen.

Anhang

Glücklicherweise erkennen wir schüchterne Anfänge von Aktivitäten, die auf konkrete Handlungen hoffen lassen:

Liste bekannter Initiativen zur Regulierung der Digitalisierung:

Alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression bei der UN Generalversammlung vom August 2018

Die **Toronto Declaration** vom Mai 2018 von Amnesty International und Access Now: *Protecting the right to equality and non-discrimination in machine learning systems* fordert auf der Basis der UN-Menschenrechte Gleichbehandlung, die Verhinderung von Diskriminierung und die Förderung von Diversität und Inklusion. Betont wird, dass Staaten beim Einsatz von maschinellem Lernen alle Menschenrechte befolgen müssen, dabei die Risiken einschätzen, Transparenz und Rechenschaftspflicht sichern, ihrer Aufsichtspflicht nachkommen und Regeln für die Privatwirtschaft erlassen müssen. Der private Sektor ist zu einer Menschenrechts „Due Diligence“ zu verpflichten, die mögliche Diskriminierung verhindert und jedermann ermöglicht, sein Recht auf gerichtliche Klage und Entschädigung durchzusetzen.

HRBA@tech: International Report *Towards A Human Rights-Based Approach to New and Emerging Technologies.*

European democracy shield: Initiative des Europäischen Parlaments vom Juni 2025. Der Anteil der Weltbevölkerung, die in demokratisch regierten Staaten leben, hat sich seit 2004 von 51% auf 28% in 2024 fast halbiert. Dagegen hat Europa bereits einige Maßnahmen ergriffen:

- Digital Services Act (DSA) regulation of online platforms and search engines,
- Artificial Intelligence Act with its risk-based approach to regulating AI, including generative AI-facilitated information manipulation such as deepfakes;
- European Media Freedom Act,
- Regulation on Transparency and Targeting of Political Advertising;
- Anti-SLAPP (strategic lawsuits against public participation) Directive.
- EuroStack: European Alternative for Digital Sovereignty, Programm zur Reduktion der Abhängigkeit von US-IT-Konzernen.

Auch im Bereich der europäischen Medien machen sich langsam Initiativen gegen die antidemokratischen, radikalisierenden und spaltenden Funktionen profitgetriebener Kommunikationsplattformen und für eine Reduktion der Abhängigkeit von amerikanischen IT-Konzernen bemerkbar:

Liste von Initiativen im Medienbereich:

- **Vom «profit space» zum «public space»:** Vorschläge zum Aufbau demokratischer digitaler Medien als Alternative zu US-Medienplattformen von der Eidgenössischen Medienkommission EMEK
- **FastForward:** Digitale Innovation öffentlich-rechtlicher Medien in Europa, veröffentlicht von ORF Public Value
- **Perspektiven für Digitalen Public Value** im ZDF
- **USETHENEWS:** Studie zur Nachrichtenkompetenz Jugendlicher und junger Erwachsener in der digitalen Medienwelt
- **European Perspective connects Europe through trusted news:**
„is a unique technical and editorial collaboration driven by trusted public service media and other public service organizations that share editorial values and high levels of public trust.“

Eine allgemeinverständliche und konkrete Leitlinie für unsere digitale Zukunft bilden die **10 Regeln für die Digitale Welt** der Future Foundation, die bei einem Workshop in Göttweig, Niederösterreich im April 2025 erarbeitet wurden:

1. Erhebt digitale Technik nicht zum Selbstzweck.
2. Schreibt Maschinen keine Menschlichkeit zu.
3. Schafft Raum für Muße und analoge Begegnung.
4. Garantiert den Erhalt sozialer und demokratischer Kompetenzen.
5. Zerstört nicht die Natur für den technischen Fortschritt.
6. Behandelt Menschen nicht als bloße Datenobjekte.
7. Lasst Euch nicht Eurer menschlichen Potenziale berauben.
8. Verleugnet nicht die Grenzen der Technik.
9. Nutzt Maschinen nicht, um die Freiheit Anderer zu untergraben.
10. Verhindert Machtkonzentration und garantiert Teilhabe.

Glossar

- **Allgemeine Erklärung der Menschenrechte 1948:**
<https://www.amnesty.at/themen/menschenrechte/die-allgemeine-erklaerung-der-menschenrechte-aemr/>
- **AI-Act der Europäischen Union 2024:**
<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1689>
- **Information:** Zielgerichteter Transfer von Wissen und Ordnung vom Sender zum Empfänger, soll Veränderungen des Realitätsbildes im empfangenden System hervorrufen, Angebot zur Vernetzung und Kooperation, Verringerung von Ungewissheit, wer Knoten in Informationsnetzwerken besetzen kann, gewinnt an Macht.
- **Turing Maschine:** abstraktes Computermodell von Alan Turing, definiert einen Computer mathematisch und beweist, dass nicht alles berechenbar ist.
- **Algorithmus:** eindeutige Vorschrift zur Lösung von klar definierten Problemen aus endlich vielen, wohldefinierten Einzelschritten, Bsp.: Kochrezept, Bauanleitung, Anweisungen, Computerprogramm.
- **Computerprogramm:** in einer Programmiersprache (Python, SQL, HTML, C, ...) formulierter Algorithmus, besteht aus Variablen (Namen für Daten-Speicher), Operatoren(=, +, -, /, *, **, >, &, (,), ...) und Funktionen (Programmteile, die vordefinierte Aufgaben erledigen).
- **Profiling:** über einzelne Personen werden aus vielen Quellen Daten gesammelt und zu Einflussnahme auf politische Entscheidungen oder Kaufverhalten genutzt.
- **Maschinelles Lernen:** Ein Lernalgorithmus baut aus vorgegebenen Beispieldaten ein mathematisch statistisches Modell auf, das dann für neue Daten Vorhersagen treffen oder Entscheidungen generieren kann.
- **Big Data:** Verfahren zum effektiven und effizienten Speichern, Verknüpfen und Auffinden riesiger Datenbestände.
- **Smartphone:** Mobiltelefon (Handy) mit Computerfunktionen und Internetanbindung, 2 Produktgruppen: Android (Google) und iPhone (Apple).
- **NLP:** Neurolinguistisches Programmieren, spezielle Kommunikationstechnik, die die psychischen Abläufe im Menschen beeinflussen sollen.

Literatur

- Alan Turing, Computing Machinery and Intelligence, Reclam, 2023
- Carolin Amlinger, Oliver Nachtwey, Zerstörungslust, Suhrcamp, 2025
- Daniel Kahneman, Thinking, Fast and Slow, Penguin, 2013
- David Chalmers, Reality+, Penguin, 2023
- Günther Anders, Die Antiquiertheit des Menschen I, II, Beck, 2002
- Hannes Werthner, Introduction to Digital Humanism, Springer, 2024
- Helga Nowotny, Zukunft braucht Weisheit, Matthes & Seitz, 2026
- Jason Hickel, Weniger ist mehr, Oekom, 2022
- Joachim Bauer, Realitätsverlust, Heyne 2023
- Jonathan B. Postel et al., A Brief History of the Internet, CoRR cs.NI, 1999
- Joseph Weizenbaum, Die Macht der Computer und die Ohnmacht der Vernunft, Suhrkamp, 1978
- Karl Polanyi, The Great Transformation, Suhrkamp, 1973
- Luke Kemp, Goliath's Curse The History and Future of Societal Collapse, Penguin, 2025
- Marietje Schaake, The Tech Coup: How to Save Democracy, Princeton, 2025
- Martin Warnke, Martin Woesler, Sozialkybernetik, Matthes & Seitz, 2024
- Max Fisher, The Chaos Machine, Quercus, 2023
- Michael Inden, Python lernen - kurz & gut, Dpunkt, 2023
- Philipp Hübl, Moralspektakel, Siedler, 2024
- Platon, Gesammelte Werke, Anaconda, 2019
- Ray Kurzweil, The Singularity is Nearer. When We Merge with AI, Viking, 2024
- Rupert Nagler, Entwurf und Realisierung von Dialogsystemen, Diss. TU Wien, 1980
- Shoshana Zuboff, Das Zeitalter des Überwachungskapitalismus, Campus, 2018
- Stephen Budiansky, Kurt Gödel und die Krise der Mathematik, Propyläen, 2022
- Tim Berners-Lee, Weaving the Web, Harper, 2020
- Viktor Mayer-Schönberger and Kenneth Cukier, Big Data, Murray, 2013
- Yanis Varoufakis, Technofeudalism, Vintage, 2024
- Yuval Noah Harari, Nexus, Penguin, 2024

Erreichbarkeit für Ergänzungen und Diskussion

nagler@idi.co.at

<https://www.allewohlstand.org/>

Link zum [Impressum](#)

Dieses Projekt wurde von der Österreichischen Gesellschaft für Politische Bildung gefördert. <https://www.politischebildung.at/>

