Grundzüge einer linken Digitalpolitik

Gruppe Die Linke im Bundestag

17.12.2024

1. Linke Digitalpolitik in der Übersicht

Die großen Chancen der Digitalisierung könnten in der Erleichterung von beschwerlicher Arbeit, dem Abbau von räumlichen und sozialen Barrieren sowie mehr Demokratie und Bildung für alle durch Transparenz, Wissenszugang und Beteiligungsprozesse liegen. Die Linke sieht sich in der Digitalpolitik in erster Linie den Interessen der Menschen verpflichtet, die in der immer stärker digital vernetzten Gesellschaft jedoch nicht nur neue Möglichkeiten erhalten. Sie werden auch neuen Hürden und Gefahren ausgesetzt, die wesentlich dadurch verstärkt werden, dass sich die Digitalisierung unter kapitalistischen Wirtschaftsverhältnissen abspielt. So entstanden gigantische digitale Monopole, wuchsen Abhängigkeiten und soziale Spaltungen, kamen immer neue Überwachungstechnologien in Einsatz. Wir wollen die Gestaltung der Digitalisierung den Profitinteressen der Konzerne entziehen. Denn wem die Digitalisierung nützt, wird jetzt entschieden.

Hürden der digitalen Teilhabe können dabei sein:

- **technischer Art**, wenn beispielsweise ein Breitbandanschluss und damit der Zugang zu schnellem Internet nicht verfügbar ist,
- **finanzieller Art**, wenn beispielsweise ein angemessener Breitbandanschluss sowie digitale Endgeräte für eine Familie mit schulpflichtigen Kindern nicht erschwinglich bezahlbar sind,
- **organisatorischer Art,** wenn Behörden nicht durch barrierefreie, digitale Angebote, auch in einfacher Sprache rund um die Uhr erreichbar sind. Oder wenn staatliche Leistungen ausschließlich digital angeboten werden und so Menschen einschränken, die einen digitalisierten Prozess nicht nutzen können oder wollen.

Gefahren der Digitalisierung bestehen bezogen auf:

- die **Beschäftigten**, beispielsweise durch die Missachtung des Beschäftigtendatenschutzes bei unerlaubter Videoüberwachung, zunehmender Leistungsüberwachung sowie enorm wachsende Flexibilisierungsanforderungen bei gleichzeitiger Verschlechterung der Mitbestimmung z.B. bei Plattformarbeit oder durch Outsourcing von Tätigkeiten wie Inhalte-Moderation oder Glasfaserkabelverlegung und dem damit einhergehenden Ausbau des Niedriglohnsektors,
- die **Nutzenden**, die in “sozialen” Medien zu Suchtverhalten durch Maximierung der Verweildauer auf Plattformen verleitet werden; es kommt zu stärkerer Konsumorientierung und Meinungsmanipulation durch gezielte Werbung bis hin zur

Desinformation und zur massenhaften Verwertung persönlicher Daten als Geschäftsmodell von Internetkonzernen, aber auch durch Kriminelle und staatliche Begehrlichkeiten,

- den **Staat**, der durch zunehmende Abhängigkeit von nichteuropäischen und privaten digitalen Diensten seine Souveränität riskiert, hinzu kommen Gefahren für die Steuergerechtigkeit, da Internetkonzerne wie Microsoft und Amazon kaum Steuern in Europa zahlen, obwohl ein wichtiger Teil ihres Umsatzes in Europa erfolgt,
- die **Ökologie**, z.B. weil Digitalisierung den Energie- und Ressourcenverbrauch enorm steigert und elektronische Geräte zu wenig repariert, nachgenutzt und recyceled werden.
- die **lokale Wirtschaft**, die von Digitalkonzernen unter Druck gesetzt wird, weil diese in die Märkte vieler klassischen Branchen immer stärker eindringen und ihre Marktmacht missbrauchen,
- **alle Bereiche** mit Bezug auf die IT-Sicherheit, denn kriminelle oder fremdstaatliche Angriffe auf IT-Systeme, z.B. als Ransomware Attacken (Daten verschlüsselt und die Herausgabe von Geld erpresst), werden immer häufiger und gefährden insbesondere kritische Infrastrukturen.

Wesentliche Ziele linker Digitalpolitik sind:

zum Abbau von Hürden der Teilhabe:

- **technischer Art**: Ausbau und Nutzung von Glasfaser- und Mobilfunknetzen mit guter Versorgung aller Haushalte und Flächen als oberste Priorität. Die Netze müssen gemeinsam von allen Anbietern genutzt werden können und sind als Bestandteil der Grundversorgung zu sehen. Unnötigen Parallelausbau durch konkurrierende Anbieter lehnen wir hingegen ab, denn das ist unnötig teuer, verschwendet Baukapazitäten, führt zu unsinnig vielen Baustellen und schadet dem Umweltschutz,
- **finanzieller Art**: Wir wollen ein Recht auf einen erschwinglichen Internetzugang, der auch das durchschnittliche Datenvolumen von Familienhaushalten abdeckt. Das Bürgergeld muss so bemessen werden, dass es ausreicht, die üblichen IT-Geräte zu kaufen,
- **organisatorischer Art**: Mit barrierefreien digitalen Angeboten und leichter Sprache muss der Staat für die Menschen jederzeit gut verfügbar sein, ob für Erledigungen in Behörden oder Möglichkeiten der Einsicht und Teilhabe am staatlichen Handeln. Die digitalen Angebote staatlicher Stellen in Deutschland hinken im internationalen Vergleich hinterher. Das könnte geändert werden, wenn auf einheitliche und offene Standards sowie freie Software gesetzt wird, sodass alle Behörden automatisch miteinander “sprechen” können, nur wenig Lizenzgebühren zahlen müssen und neue Entwicklungen nur einmal gemacht und dann gemeinsam genutzt werden können. Gleichzeitig gibt es immer Gründe, warum Menschen mit staatlichen Stellen, der Post, der Bahn oder der Ärztin nicht online kommunizieren können oder wollen. Diese Wege müssen langfristig, kostenlos und ohne Nachteile für den Einzelnen möglich bleiben. Dafür müssen Anlaufstellen wie Bürgerbüros zur Antragstellung und Beratung weiterhin offline verfügbar sein. Chipkarten wie die Gesundheitskarte oder der Personalausweis müssen dauerhaft erhalten bleiben und den Zugang zu allen benötigten Leistungen ermöglichen. Auch die Bezahlung mit Bargeld muss möglich bleiben.

zur Bewältigung von Gefahren der Digitalisierung:

- **für Beschäftigte:** Bei beruflichen Tätigkeiten, die durch Digitalisierung ersetzt werden könnten, muss kritisch geprüft werden, ob dadurch die Produkte und Dienstleistungen an Qualität verlieren, etwa an Schulen, im Gesundheits- und Pflegesektor, aber auch im Bereich der Kultur- und Kreativwirtschaft. Digitalisierung als Sparmaßnahme auf Kosten der Beschäftigten und zulasten der Nutzenden lehnen wir strikt ab. Stattdessen sollen Digitalisierungsmaßnahmen zur Verbesserung von Arbeitsbedingungen führen. Digitalisierung darf nicht als Vorwand zu einseitiger Flexibilisierung und Ausdehnung der Arbeitszeiten durch ständige Erreichbarkeiten genutzt werden. Wir fordern eine verbindliche Arbeitszeiterfassung und ein Recht auf vom Arbeitgeber bezahlte Weiterbildung, damit zum Beispiel der Aufbau digitaler Kompetenzen in der Breite besser gefördert wird. Dass sich linkes Engagement in Parlamenten auszahlen kann, zeigt die EU-Richtlinie zu Plattformarbeit, die Beschäftigte von Onlineplattformen besser vor Ausbeutung schützen soll – auch wenn es auf ihre Umsetzung ankommt. Vor allem Crowdworkerinnen und Crowdworker unterliegen nach wie vor oft prekären Arbeitsbedingungen. Wir bevorzugen Internetwirtschaft in Gemeineigentum oder in der Hand der Beschäftigten, um der zunehmenden Konzentration von Einkommen und Vermögen entgegenzuwirken. Wir streiten für eine solidarische Globalisierung, die Beschäftigten und Verbrauchern weltweit ökologische und soziale Standards sichert. Deshalb haben wir das EU-Lieferkettengesetz unterstützt und setzen uns in internationalen Handelsverträgen u.a. dafür ein, dass die Produktion von Hardware für die digitale Kommunikation unter menschenwürdigen Bedingungen erfolgt. Das darf nicht nur unverbindlich gefordert werden: Es muss kontrolliert und nachvollziehbar für Verbrauchende zertifiziert werden. Auch in Deutschland darf Digitalisierung nicht auf dem Rücken der Beschäftigten vorangetrieben werden – das Geflecht aus Subunternehmer-Ketten beim Glasfaserausbau führt zu Entrechtung und massiver Ausbeutung der Bauarbeiter, und Content-Moderierende für soziale Netzwerke arbeiten selbst hierzulande teilweise unter unvertretbaren Zuständen, für mehr Profit bei Digitalkonzernen. Der Schutz der Privatsphäre muss auch für Beschäftigte gelten. Im Job entstehen eine Vielzahl von personenbezogenen Daten, die erhoben, verarbeitet und ggf. auch gelöscht werden müssen - egal ob im Büro, bei Lieferdiensten, im Einzelhandel oder der Logistikbranche. In Zeiten von komplexen und selbstlernenden Algorithmen und Big Data braucht es klare und transparente Regeln zum Schutz von Beschäftigtendaten. Doch noch immer sind viele Bestimmungen zu vage formuliert und so entscheiden seit Jahren vor allem Gerichte einzelfallbezogen. Wir fordern deshalb ein starkes Beschäftigtendatenschutzgesetz, das die Mitbestimmung der Betriebsräte ausbaut und für alle Beschäftigten gilt,

- **für Nutzende:** Wir fördern werbefreie Plattformen, Software und Netzwerke in der Hand der Nutzenden und Plattformen in gemeinnütziger Trägerschaft. Es gibt bereits gute Praxisbeispiele dafür: Das Lexikon Wikipedia, die sozialen Netzwerke Mastodon und Bluesky, das Betriebssystem Ubuntu, der Internetbrowser Firefox, der AppStore F-Droid oder die KI-Software StableDiffusion. Dadurch schwächen wir die von Datensammelwut und Lizenzgebühren getriebenen Geschäftsmodelle des digitalen Kapitalismus. Auf diese Weise wird nicht nur Umverteilung von unten nach oben verlangsamt und die Ausbeutung der Nutzenden durch Suchtauslösung und Herausgabe persönlicher Daten gestoppt, sondern gleichzeitig die freie Meinungsbildung gestärkt und echte digitale

Selbstbestimmung ermöglicht. Parallel stärken wir das Können des Umgangs mit Internetmedien für alle: Zum Erkennen von Desinformation und Deep Fakes, zum Einstellen von Privatsphäre-Optionen, oder um Software gut anpassen oder sogar aktiv verändern zu können. Es braucht eine konsequente Umsetzungskontrolle gesetzlicher Auflagen an Onlinedienste wie Nutzungsfreundlichkeit, Transparenz und wirksame Melde- und Einspruchsmöglichkeiten bei Verstößen z.B. gegen Persönlichkeitsrechte oder bei Betrug. Selbstverständlich kämpfen wir auch gegen Abo-Fallen mit finanziellen Schäden sowie gegen Daten- oder Identitätsdiebstahl,

- **für Staatliche Stellen** Um seine Souveränität und gleichzeitig Transparenz zu wahren, muss der Staat seine digitale Infrastruktur einschließlich von Clouds selbst und soweit möglich unabhängig von Dritten mit freier Software und offenen, einheitlichen Standards betreiben. Dafür sind gemeinsame Entwicklungsplattformen und öffentliche Betriebe wichtig. Das nützt allen, weil freie Software überall nachgenutzt, angepasst und weiterentwickelt werden kann. Auch baut der Staat so mehr eigene IT-Kompetenz auf und wird funktionsfähiger und resilienter. Die Zusammenarbeit mit Unternehmen, die gesetzlich zur Herausgabe von Daten an nichteuropäische Behörden verpflichtet werden können, ist konsequent abzulehnen und gefährdet nicht nur die staatliche Souveränität, sondern auch die Persönlichkeitsrechte der Einwohnenden. Auch staatliche Interessen führen zu Gefahren für Privatsphäre, Meinungsfreiheit und IT-Sicherheit. Wir streiten für einen starken Schutz privater Inhalte in Messengern, Emails, Clouds und sozialen Netzwerken.
- Netzsperren und eine zunehmende Ausweispflicht im Internet lehnen wir als unpräzise Maßnahmen mit hohen Risiken für die Grundrechte ab. Der Staat darf keine digitalen Hintertüren zum Spionieren offenhalten, sondern muss deren Schließung unmittelbar veranlassen. Wenn der Staat aus legitimen Gründen gegen Personen ermitteln muss, hat das auch im digitalen Raum mit Methoden zu geschehen, die die IT-Sicherheit und Persönlichkeitsrechte nicht über den konkreten Ermittlungsfall hinausgehend beschädigen,

- **für die Ökologie:** Der Netzausbau ist am umweltschonendsten, wenn ein gemeinsames Netz gebaut wird, das alle nutzen können, anstatt mehrerer Netze nebeneinander. Befreit vom werbe- und datenbasierten Geschäftsmodell vieler Internetkonzerne wäre der Energieverbrauch vieler Dienste und Apps viel niedriger. Mehr technische Standards und offenes Design könnten eine Menge nicht passender Teile vermeiden und Geräte vielseitiger und länger nutzbar machen. Kernkraft und fossile Energieträger sind große Gefahren für den Umwelt- und Klimaschutz, doch selbst die Erzeugung regenerativer Energien belastet die Umwelt. Deshalb ist und bleibt Sparsamkeit enorm wichtig. Auf den Einsatz energiehungriger Software wie künstliche Intelligenz oder Blockchain sollte verzichtet werden, wenn sich die adressierten Probleme auch einfacher lösen lassen. Hersteller müssen dazu verpflichtet werden, IT-Geräte lange nutzbar und gut reparier- und recycelbar zu produzieren. An Kosten der Reparatur und Verwertung müssen sich Hersteller in einem Maße beteiligen, dass sich der Verkauf neuer Produkte nur noch lohnt, wenn diese nachhaltig konzipiert sind. Die Forschung zum Ersatz seltener Rohstoffe durch gut verfügbare, umweltverträglichere Materialien für die Digitaltechnik wollen wir verstärken,

- **für die Wirtschaft**: Der Erfolg der Wirtschaft sollte sich auch daran messen lassen, ob sie den sozialen Zusammenhalt stärkt und den Umweltschutz sicherstellt. In dem von uns angestrebten Ökosystem aus offenen Standards, freier Software und hoher Verfügbarkeit öffentlicher und ökonomischer Daten könnte sich eine neue Digitalwirtschaft besser und kollaborativer entwickeln. Auch hilft es europäischen Unternehmen, wenn sie Entwicklungs- und Dienstleistungsaufträge erhalten, die sich gegenwärtig nichteuropäische Großkonzerne einverleiben, die keinen glaubhaften Datenschutz gewährleisten können. Digitalkonzerne müssen sich endlich angemessen am Steueraufkommen in Deutschland und Europa beteiligen. Der IT-Fachkräftemangel ist und bleibt groß, weshalb eine umfassende Weiterbildungsoffensive wichtig ist. Entscheidend sind nicht unbedingt weit überdurchschnittliche Gehälter, sondern vielmehr ein Arbeitsplatz, der gute Arbeit und soziale Sicherheit ebenso bietet, wie Mitbestimmungsmöglichkeiten und eine hohe Identifikation mit dem Arbeitsziel. Gerade dafür bietet (digitale) Gemeinwohlwirtschaft besonders günstige Voraussetzungen,

- **für alle Bereiche:** Die IT-Sicherheit für alle lässt sich u.a. durch die Förderung von Open Source Software (Entwicklung und Pflege), durch die konsequente Schließung aller bekanntwerdenden bzw. gewordenen Schwachstellen, durch ein gut ausgestattetes und unabhängiges Bundesamt für Sicherheit in der Informationstechnik (BSI), aber auch durch eine Stärkung der IT-Sicherheitskompetenz in der ganzen Gesellschaft erhöhen. Sicherheitsforschung muss entkriminalisiert und besser finanziert werden, BSI Grundschutz-Standards müssen auch für Kommunen gelten, die wie KMU in der Umsetzung Unterstützung benötigen. Verbindliche IT-Sicherheitsstandards braucht es gerade mit Blick auf kritische Infrastrukturen.

2. Digitale Technologien in Gegenwart von Kapitalismus und weiteren Krisen

Die Gesellschaft in Deutschland, Europa und weltweit ist vielfältigen Krisen ausgesetzt: Soziale Ungerechtigkeit und damit verbundene Verluste bei Vertrauen und Zusammenhalt haben sich vermehrt, die Klimakrise wurde verschärft, und es wird ein Krieg in Europa und auch andernorts geführt. Gleichzeitig wird die Gestaltung unserer digitalen Gesellschaft weiterhin vor allem von internationalen Großkonzernen, diversen Milliardären und ihren einseitigen privatwirtschaftlichen Interessen geprägt. Daraus resultieren eine Vielzahl von Widersprüchen:

- der Widerspruch zwischen dem Charakter digitaler Ressourcen, die eine freie Nutzung durch die Gemeinschaft ermöglichen, und ihrer privat- und eigentumsrechtlichen Aneignung durch Wenige, die absurde Reichtümer anhäufen und wie Elon Musk ihre Milliardärsmacht auch für politischen Einfluss zum Nachteil des Gemeinwohls missbrauchen,
- der Widerspruch zwischen angeblich rechtlich gleichen Akteuren und einer Realität von digitalen Monopolen, die allgemein unter dem Label „Plattform-Kapitalismus“ beschrieben werden,
- der Widerspruch zwischen Effizienzgewinnen und einem gerade dadurch induzierten Mehrverbrauch an Ressourcen, der neben Treibhauseffekten auch den ausbeuterischen Verbrauch „seltener Erden“ und anderer Rohstoffe, wie Kobalt oder Gold bei der Produktion von Hardware zufolge hat,

- der Widerspruch aus potenziell interoperabler, freier Software, offenen Standards und maximaler Transparenz und einer Abschottung durch den technischen wie lizenzrechtlichen Aufbau von Lock-In Effekten, die allein der Profitmaximierung und dem Ausbau proprietärer Ökosysteme dienen,
- der Widerspruch aus Informationsgesellschaft und Informationsverknappung, Closed-Source-Software statt Open-Source-Software, restriktive Lizenzen, Netzsperren und Zensur statt digitale Commons, personalisierte Werbung statt freie Meinungsbildung, digitale Konsumtempel statt neutrale Handelsplattformen, Sucht-induzierende Plattformen statt echte soziale Netzwerke.

Es wird zwar versucht, mit gesetzlicher Regulierung vor allem auch auf EU-Ebene gegenzusteuern. Diese Regelwerke bleiben jedoch durch finanzstarken Wirtschaftslobbyismus löchrig. Anstatt ausbeuterische Geschäftsmodelle zu stoppen, wird mit Steuertricks jongliert, Arbeitskräfte in den Niedriglohnsektoren ausgelagert, und den Nutzenden wird die scheinbare Freiheit gegeben, in die Geschäftsmodelle der Anbietenden freiwillig einzuwilligen (z.B. Cookie-Banner). In der Praxis werden Nutzende durch irreführende Designs, die eine bestimmte Entscheidung bereits nahelegen („Dark Patterns“), durch Koppel-Verträge mit Produkten (mit Kauf von Produkt X erfolgt automatisch Einwilligung in Datennutzungsverträge) und Datenkapitalismus (bezahle mit Geld oder mit deinen Daten) zu deutlich mehr Preisgabe persönlicher Daten verleitet, als den Betroffenen bewusst ist, und das Persönlichkeitsrecht systematisch unterwandert. Verbraucherinnen und Verbraucher können keinen wirklich informierten Überblick darüber gewinnen, welche Daten für welche (Werbe-)zwecke wo und wann genutzt werden und wie sich das durch Werbeanzeigen auf ihre Meinungsbildung auswirkt. Und während Menschen die Verletzung ihrer Persönlichkeitsrechte in sozialen Medien oder im Beruf oft ohnmächtig ertragen müssen, wird gegen die Verletzung von Eigentumsrechten wie Urheberrechte sowie gegen politisch unerwünschte Inhalte mit unverhältnismäßiger Überwachung, Abmahnungen und weitreichenden Zensurmaßnahmen wie Netzsperren vorgegangen.

Die Datenschutz-Grundverordnung (DSGVO) war ein wichtiger Schritt. Ihr Ziel war es aber nicht, die Macht der Plattformen zu brechen und der Kommerzialisierung unseres digitalen Lebens Schranken zu setzen. Bei besonders wichtigen Vorgaben, etwa zum Transfer von Daten in Drittländer, fehlt es an effektiver Durchsetzung. Eine datenrechtliche Regulierung, die das Gemeinwohl zum Ziel hat, muss die Datenverarbeitung konsequent in den Dienst der Menschen stellen und die Ökonomisierung des digitalen Lebens, aber auch ihre Ausnutzung zu staatlicher Massenüberwachung mit digitalen Methoden verhindern. Bei der Regulierung Künstlicher Intelligenz in der KI-Verordnung der EU werden diese Ziele verfehlt, da sie z.B. biometrischer Identifikation im öffentlichen Raum Tür und Tor öffnet und wirtschaftliche Freiheit sowie staatliche Interessen stärker berücksichtigt als Schutzrechte von Menschen.

Überwachung, das Sammeln personenbezogener Daten und Kontrolle durch staatliche Stellen und Internetkonzerne nehmen zu, weil es nicht nur dem Ankurbeln von noch mehr Konsum „nützt“, sondern auch der Durchsetzung hoheitlicher Interessen. Nach den eindrücklichen Leaks von Edward Snowden im Jahr 2013 und dem Handeln zahlreicher autoritär geprägter Staaten konnte in Europa zwar mehr Transportverschlüsselung umgesetzt werden, jedoch fand kein ausreichender Sinnes- oder gar Strukturwandel statt. Im Angesicht von Plänen der „Chatkontrolle“, Staatstrojanern, Vorratsdatenspeicherung, automatisierter biometrischer

Fernidentifizierung und fortbestehenden US-Spionage-Rechtsakten, von denen der CLOUD-Act nur ein Beispiel ist, werden europäische Grundrechte, die informationelle Selbstbestimmung, „privacy by default“ und das Recht auf Anonymität immer wieder unterlaufen.

Digitale Technologien werden rasant weiterentwickelt und unermüdlich als Lösung für Probleme und Krisen angeboten, selbst dann, wenn sie gar keine technische, sondern eine gesellschaftspolitische Problemlösung erfordern. Mit Hype-Technologien werden Heilsversprechen verbunden, sodass z.B. Vorhaben auf der Basis von Blockchain Technologie oder Künstlicher Intelligenz mit enormen staatlichen und auch privaten Mitteln gefördert werden, ohne die Erwartungen auch nur ansatzweise zu erfüllen. Dabei stellt uns inzwischen gerade auch generative KI vor neue Herausforderungen, die Zukunft von Medien und Journalismus steht auf dem Spiel, Deep Fakes beeinflussen gesellschaftliche Diskurse, Bildung, Forschung und Regulierung halten kaum Schritt mit diesen Entwicklungen. Gleichzeitig werden für überfällige gesellschaftliche Veränderungen die notwendigen Mittel nicht bereitgestellt. Gemeinwohlorientierte Anwendungen, die wirklichen Nutzen für Viele bringen würden, bleiben unterfinanziert. Negative Auswirkungen digitaler Technologien werden mit dem Argument der „Innovationsfeindlichkeit“ unter den Teppich gekehrt, der gesellschaftliche Schaden wird sozialisiert, z.B. die Folgen des Ressourcen- und Energieverbrauchs durch Kryptowährungen.

3. Notwendige strukturelle Veränderungen im Einzelnen

Veränderung 1: Ein digitales Ökosystem für Gemeinwohl und Demokratie

> *Treiber der Digitalisierung ist für uns das Gemeinwohl. Offene Standards und offene Daten, Open Source, Open Hardware und digitale Commons sind die Grundlagen dafür. Demokratie und Gemeinwohl kommen jedoch nie ohne Schutz der Persönlichkeitsrechte aus. Diese müssen technisch und rechtlich abgesichert sein. Es gilt das Prinzip „Offene Daten nützen, private Daten schützen“.*

Egal, ob zuhause oder auf der Arbeit, auf dem Dorf oder in der Stadt, wir fordern stets heraus zur Frage: Wer entscheidet, welche digitalen Technologien wo, durch wen und zu welchem Zweck entwickelt, gefördert oder verhindert werden? Die Antwort geben nicht nur Funktionstragende des Staates, sondern die Bürgerinnen und Bürger selbst – durch einfach nutzbare Werkzeuge für Petitionen, Schnittstellen für barrierearmen Austausch mit staatlichen Stellen und Online-Diskussionsformate.

Wir fordern:

- **digitale Abstimmungswerkzeuge** als Bereicherung der repräsentativen Demokratie,
- transparentes Handeln des Staates und ein **Recht auf Open Data** als Wissensgrundlage für informierte Teilhabe. Das Prinzip des gläsernen Staates ist auch die Voraussetzung dafür, dass Korruption und verfehlte Investitionen erkannt und korrigiert werden können,

- eine **digitale Infrastruktur gehört in öffentliches Eigentum** – von Glasfasernetzen bis zum Funkmast, denn sie müssen Teil der Daseinsvorsorge sein und flächendeckend Teilhabe sicherstellen, auch in abgelegenen Dörfern,
- eine **Digitale Identität**, die eine Identifizierung im Internet auf das Minimum beschränkt, das unvermeidlich ist, um sich auszuweisen und Rechte durchzusetzen. Das Recht auf Anonymität auch im öffentlichen Raum, etwa in sozialen Netzwerken, ist zu wahren. Gleichzeitig muss die Infrastruktur der digitalen Identitäten unter öffentlicher Kontrolle stehen, denn nur dann ist ihre Anwendung zur Rechtsdurchsetzung legitim. Das gilt beispielsweise für die Bekämpfung von Finanzkriminalität oder zum Schutz vor digitaler Gewalt. Auch die elektronische Patientenakte und dazugehörige Apps sind gemeinnützig von der öffentlichen Hand zu betreiben und dürfen keinen Profitinteressen ausgesetzt werden,
- eine **soziale Infrastruktur der digitalen Gesellschaft** – wichtige Dienste, ohne die man kaum an ihr teilhaben kann – die auch nicht-kommerziell verfügbar sind. Sie werden entwickelt und betrieben z.B. von Genossenschaften, öffentlich-rechtlichen Anstalten, Stiftungen, Bürgerinitiativen, Vereinen oder staatlichen Institutionen. Wenn mögliche staatliche Kontrolle unerwünscht ist, ist immer auf Staatsferne zu achten,
- **ein offenes soziales Netzwerk auf EU-Ebene**, das gemeinnützig und vor privater wie staatlicher Übergriffigkeit strukturell geschützt ist, von Nutzenden verwaltet wird, keinem anderen Zweck als der Vernetzung von Menschen dient und maximalen Anforderungen an Transparenz, Offenheit und Nutzenden-Autonomie genügt,
- den Schutz der Meinungsfreiheit als hohes, weitreichendes Gut. Löschpflichten darf es nur für strafbare Inhalte geben,
- **ein offenes, gemeinwohlorientiertes KI-Ökosystem**, das in Einklang mit den Grundrechten steht und soziale sowie ökologische Nachhaltigkeit gewährleistet, um ein Gegengewicht zur extremen Machtkonzentration durch einige wenige kommerzielle Akteure zu schaffen,
- gute Entwicklungsbedingungen für **werbefreie Plattformen, Software und Netzwerke** in Gemeineigentum. Wege der Finanzierung sind öffentliche Förderung benötigter Infrastruktur und Basisdienste, die sehr preiswert nutzbar sein müssen. Spenden für Plattformen im Gemeineigentum müssen rechtlich begünstigt und steuerlich noch bessergestellt werden. Einnahmen aus der stärkeren Besteuerung von Internetkonzernen können zur zusätzlichen Förderung herangezogen werden, um die antikapitalistische Transformation der digitalen Gesellschaft zu beschleunigen. Entwickelnde und Anbietende nicht-kommerzieller Dienste wie z.B. der Fediverse-Plattform Mastodon sollten grundsätzlich als gemeinnützig anerkannt werden können,
- **Internetzugang für alle:** Wir fordern einen erschwinglichen Internetzugang flächendeckend und für Alle; die konsequente Verteidigung der Netzneutralität; Barrierefreiheit und leichte Sprache bei Verwaltungsdiensten,
- **kein Digitalzwang**: Waren und Dienstleistungen, auf die Bürgerinnen und Bürger im Alltag angewiesen sind, dürfen nicht an die zwingende Nutzung von Apps gekoppelt sein und müssen stets auch offline in Anspruch genommen werden können. Der elektronische Personalausweis mit Chipkarte muss als Identitätsanker erhalten bleiben. Außerdem setzen wir uns für ein Recht auf Bargeldnutzung ein, da es nicht nur digitale Zahlungsmittel geben darf,
- **Grenzen** für den Einsatz digitaler Technologien, wenn die Nachteile für Umwelt und Mensch den gesellschaftlichen Nutzen unangemessen übersteigen. Dazu wollen wir mehr offene, gesellschaftliche Debatten zur sozial-ökologischen Transformation und

Formulierung von Visionen: In welcher Gesellschaft wollen wir leben und welche Technikfolgen müssen wie beachtet werden?

Veränderung 2: Die Macht von Digitalkonzernen konsequent begrenzen

Wir fordern:

- **die Zerschlagung digitaler Monopole von Konzernen.** Solange Monopolisten existieren, müssen sie wenigstens angemessen am Steueraufkommen beteiligt werden: Wir fordern einen globalen Mindeststeuersatz von 25 Prozent, eine Digitalsteuer, die Umsätze dort versteuert, wo sie generiert werden und eine Übergewinnsteuer für Krisengewinner wie Amazon während der Corona-Pandemie. Zudem braucht es ein konsequentes Verbot von Dark Patterns und von personalisierter Onlinewerbung, gut erreichbare Meldefunktionen bei Verletzungen der Persönlichkeitsrechte durch Nutzende, Sicherstellung von Interoperabilität seitens des größeren Marktteilnehmenden und ein umfassender Informationszugang zu Plattformdaten für Forschende. Die zuständige(n) Aufsichtsbehörde(n) in Deutschland (z.B. die Bundesnetzagentur für den Digital Services Act) sind ausreichend auszustatten, um ihre Aufgaben effektiv und umfassend wahrnehmen zu können. Strukturelle Verstöße müssen mit empfindlichen Strafzahlungen geahndet und diese notfalls mit gezielten polizeilichen Ermittlungen durchgesetzt werden. Verbote ganzer Plattformen und weitreichende Verpflichtungen zur Datenausleitung an Behörden lehnen wir hingegen ab,
- keine Digitalisierung auf Kosten **guter Arbeit** und Daseinsvorsorge. Vorgabe und Kontrolle sozialer und ökologischer Standards in der gesamten Lieferkette und Produktion,
- **Datenschutz ohne Dateneigentum**: Der Schutz der Persönlichkeitsrechte darf nicht vom Geldbeutel abhängen oder von kapitalistischer Verwertungslogik ausgehebelt werden. Deshalb ist der Vorstellung von Daten als wirtschaftliches Eigentum eine klare Absage zu erteilen. Wir lehnen auch das Konzept der informierten Einwilligung in diese Verwertungslogik (zum Beispiel durch Cookie-Banner) ab. Eine solche Einwilligung ist in überschaubaren Grenzen, etwa beim Teilen von Gesundheitsdaten zu gemeinnützigen Forschungszwecken legitim, nicht jedoch für den Werbemarkt.

Veränderung 3: Digitalkompetenzen aufbauen

Die Krisen unserer Zeit als auch der technologische Fortschritt erfordern für einzelne Personen und auch für die gesamte Gesellschaft ganzheitliche Visionen und ein neues Denken. Die Voraussetzung hierfür ist neben einem klaren Fokus der Forschung zu Langzeitwirkung auch die Befähigung und das Verstehen von Geräten und Anwendungen in unser aller Alltag. Angefangen bei der Schule bis hin zur politischen Entscheidungsebene geht es nicht nur darum, was mit digitaler Technologie erreicht werden kann, sondern auch darum, wer sie zu welchem Zweck und mit welcher Wirkung auf die Umwelt, unsere Gesellschaft und uns als Individuen einsetzt.

> *Staatliche Kompetenzdefizite sind ein Problem. Bund und Länder setzen oft auf externe Beratungsfirmen, statt eigene Kompetenzen aufzubauen. Die Folge sind oft schlechte Ausschreibungen mit überteuerten und ungeeigneten Angeboten. Viele IT-Projekte und die Digitalisierung der Verwaltung scheitern am internen Kompetenzmangel.*

Wir fordern:

- **öffentliche Gelder für öffentliche Güter:** Diese Maxime linker Datenpolitik ist durch aktive Schutzmaßnahmen vor Wirtschaftslobbyismus, Aufbau von Kompetenz innerhalb der öffentlichen Hand und gezielte Schulungen und Weisungen in der Vergabepraxis umzusetzen. Die Maxime besagt, dass öffentliches Geld ausschließlich in Software und Daten/Informationen investiert wird, die potenziell frei nachnutzbar und anpassbar sind, an denen niemand Eigentumsrecht geltend machen kann und die zu keinen starken Abhängigkeiten gegenüber einzelnen Akteuren führen können. Beispielsweise erteilen wir der Entwicklung und dem Betrieb der IT staatlicher Stellen durch proprietäre Software von Microsoft, Google, Amazon & Co eine klare Absage. Das gilt beginnend von Endnutzer-Anwendungen über Cloud-Stacks, Virtualisierungssoftware bis hinunter auf die Ebene der Betriebssysteme und Firmware,
- eine **Teilhabe** an digitaler Gesellschaft, die allen ohne Benachteiligungen und materielle oder zeitliche Barrieren möglich sein muss. Teilhabe erfordert nicht nur Zugang zur Infrastruktur und zu Geräten, sondern auch Kompetenzen,
- einen offenen Zugang zu **Wissen und Kultur**: Wir fordern umfassend Open Access für wissenschaftliche Arbeiten, ein Ende der Depublikation öffentlich finanzierter Medieninhalte und Open Educational Resources als Standard in Bildungseinrichtungen. Damit Journalismus und Kulturschaffende nicht auf künstliche Zugangsbarrieren zu digital verfügbaren Inhalten angewiesen sind, müssen erleichterte Finanzierungsmöglichkeiten über Vergütungspflichten, Spenden, öffentliches Geld und auch neue Modelle wie eine Kulturwertmark (partizipatives Beitragskonzept nach Ideen des Chaos Computer Clubs) ermöglicht werden. Bestehende Vergütungsmodelle sind gerechter auszugestalten, sodass Kreative ihre Interessen gegenüber ihren Vertragspartnern und Verwertungsgesellschaften besser durchsetzen können,
- ein **Recht auf eine vom Arbeitgeber finanzierte Weiterbildung** im Arbeitsrecht und eine Weiterbildungsoffensive für die Verwaltung: Digitalkompetenzen sind auf allen Ebenen der öffentlichen Verwaltung, insbesondere auch auf Führungsebenen und in Vergabestellen auszubauen. Wir fordern gemeinsame Entwicklungsplattformen für Software, Standards und Arbeitsprozesse,
- eine **Befähigung** zur Digital- und Medienkompetenz, die von Kindern bis hin zu alten Menschen Alle einschließt. Sie hat der Schrittmacher der Digitalisierung zu sein, nicht umgekehrt. Sie ist nicht nur der Schlüssel zu mehr Teilhabe, sondern ermöglicht auch **Schutz vor der Wirkung von Falschinformationen, Desinformation und vor digitaler Gewalt**. Sie befähigt darüber hinaus, nicht nur Dienste in Anspruch zu nehmen und zu konsumieren, sondern diese auch aktiv mitzugestalten. Warum und wie dabei Open Source, Commons und Open Data helfen, muss mit Priorität vermittelt werden.

Veränderung 4: Sichere Digitale Technologien

Die Lücken in der IT-Sicherheit von Unternehmen aller Größen sowie bei Behörden, Bildungseinrichtungen und Individuen werden immer sichtbarer, denn mit neuen technischen Möglichkeiten und immer lukrativeren, kriminellen Geschäftsmodellen oder mächtigen staatlichen Akteuren werden Angriffsszenarien häufiger und gefährlicher.

> *Menschenrechte und Medienfreiheit werden weltweit bedroht, der NSA-Skandal bleibt ohne Konsequenzen, eine Regierung nach der anderen unterstützt diverse Varianten der Massenüberwachung, die*

einhergehen mit dem Offenhalten oder sogar Einbauen von Sicherheitslücken, die von Geheimdiensten genauso wie von Kriminellen genutzt werden können. Sicherheit wird damit nicht geschaffen, sondern ausgehöhlt!

Der Schutz vor digitaler Gewalt ist sehr viel umfassender als der Schutz vor Desinformation und Hatespeech. So wird darunter auch der Schutz vor Gewalt aus dem Nahumfeld und viele weitere Gewaltformen umfasst („Revenge Porn", Cybermobbing, Cybergrooming, Cyberstalking, Doxing, Deep Fakes u.v.m.). Die Istanbul Konvention wird mit Bezug auf digitale Gewalt gegen Frauen und Mädchen bisher nicht ausreichend umgesetzt.

Wir fordern:

- eine Digitalisierung, die auf **Sicherheit** im Umgang mit Geräten, Netzen und eigenen Daten basieren muss. Dazu gehören eine Mindestupdatepflicht und eine Produkthaftpflicht für Software sowie eine Meldepflicht für Sicherheitslücken. Der staatliche Handel oder das Offenhalten von Sicherheitslücken müssen verboten werden,
- die Förderung von **Open Source** und Entkriminalisierung der **IT-Sicherheitsforschung** durch Reform des sogenannten „Hackerparagraphen", staatl. Investition in IT-Sicherheitsforschung,
- dass **Datensparsamkeit und Datensicherheit** von Beginn an zusammen gedacht, geplant und umgesetzt werden müssen – Privacy und Security by Design als Priorität, nicht als Nebenprodukt. Ende-zu-Ende-Verschlüsselung muss der Standard für private Kommunikation und private Daten auf Servern bzw. Clouds werden. Datenübermittlung an Anbietende, die aufgrund der Rechtslage anderer Staaten zur Kooperation mit ausländischen Sicherheitsbehörden verpflichtet werden können, sehen wir kritisch und ist für personenbezogene und vertrauliche Daten bei deutschen Behörden und öffentlichen Institutionen strikt abzulehnen. Staatstrojaner und andere Spähsoftware auf Endgeräten ist ausnahmslos inakzeptabel. Die Weitergabe signierter Credentials an Dritte zu hoheitlichen Ausweiszwecken ist abzulehnen und bei Ausweisvorgängen muss das Prinzip des Zero-Knowledge-Proof eingehalten werden. Das Recht auf anonyme Internetnutzung muss gewahrt bleiben. Authentische Identitätsnachweise müssen auf das absolute Minimum beschränkt bleiben,
- eine Evaluierung der **DSGVO** und ihrer Grenzen, eine Einschränkung der wachsenden Ökonomisierung des digitalen Lebens und das **Schließen regulativer Lücken**, damit gemeinwohlorientierte Datennutzung priorisiert und Nutzende effektiver vor unerwünschter Profilbildung und Manipulationen geschützt werden**.** Die bisher dominante individuelle Selbstbestimmung, bei der mit einem Einwilligungsklick alles erlaubt ist, brachte nicht die erwartete Schutzwirkung,
- dass die digitalen Möglichkeiten nicht zur **anlasslosen Überwachung** der Menschen und zur Einschränkung der Demokratie genutzt werden dürfen, der Export von Überwachungstechnologie muss verboten werden. Überwachungs- und Sicherheitsgesetze sind zu evaluieren und ihre Wirkung in einer Überwachungsgesamtrechnung zu bewerten, die Grund- und Bürgerrechte dürfen nicht eingeschränkt werden („Chilling Effekt"),
- **dass kritische Infrastrukturen** (dazu gehört unserer Auffassung nach auch die öffentliche Verwaltung bis zu den Kommunen) besser geschützt und KMU besser unterstützt werden

müssen, z.B. durch geförderte Open Source Software und Open Source IT-Sicherheitswerkzeuge und besseren Zugang zu IT-Sicherheitsexpertise, auch im Angriffsfall,
- **einen Ausbau der IT-Sicherheitskompetenzen** in der gesamten Bevölkerung,
- den Schutz vor **digitaler Gewalt** in all ihren Ausprägungen als Aufgabe der Gesellschaft einschließlich des Staates, die Istanbul Konvention muss auch für diese Gewaltformen endlich umgesetzt werden. Dazu gehört mehr als ein effektives Digitale-Gewaltschutz-Gesetz, weil es z.B. auch Prävention und Opferunterstützung braucht. Zur Bekämpfung sexualisierter Gewalt an Kindern fordern wir Pflichten zur Risikominderung seitens der Plattformen, gute Meldefunktionen, viel Aufklärungsarbeit auch zu Cyber-Grooming an Schulen, gut ausgestattete Beratungsstellen, sensibilisierte Jugend- und Polizeiarbeit und einzelfallbezogene verdeckte Ermittlungen mit OSINT-Werkzeugen und Social Engineering, um das Problem zu bekämpfen. Nicht hilfreich hingegen ist eine Kriminalisierung alterstypischer Sexualentwicklung Jugendlicher, das Ansammeln dokumentierter sexualisierter Gewalt in riesigen Datensilos zum Training darauf abgerichteter künstlicher Intelligenz und der Versuch, mit weitreichender Überwachung und Repression im Internet ein soziales Problem lösen zu wollen (Bsp. „Chatkontrolle“). Verpflichtende Altersnachweise in sozialen Netzen für den Kinder- und Jugendschutz lehnen wir ab, solange es keine technischen Lösungen gibt, die einen Datenaustausch garantieren, der auf das absolut notwendige Maß beschränkt bleibt („Zero Knowledge Proof“) und das Recht auf anonyme Internetnutzung garantiert,
- **dass Hass, Hetze und massenhafte** Desinformation nicht unseren gesellschaftlichen Zusammenhalt zerstören. Insbesondere braucht es mehr Resilienz und effektive Gegenmaßnahmen gegen strukturierte Einflussnahmen von Drittstaaten auf gesellschaftliche Debatten mit dem Ziel, das Vertrauen in demokratische Prozesse und Institutionen zu zerstören, Wahlen zu beeinflussen und uns zu spalten und zu radikalisieren. Digitale Plattformen haben dabei mehr Verantwortung zu übernehmen, z.B. um Botnetze aufzudecken und offline zu nehmen – Meinungsfreiheit ist ein Menschenrecht, also keines für Bots. Wir fordern eine Kennzeichnungspflicht für Bots und ein Verbot von Bots, die direkt oder indirekt vorgeben, ein Mensch zu sein,
- zur **Durchsetzung legitimer Gemeinwohlinteressen** wie den Kampf gegen Geldwäsche, Steuerhinterziehung, Terrorismus oder sexualisierter Gewalt notfalls auch Werkzeuge wie OSINT-tools und digitale Honey-Pots für den Staat, wenn Präventionsmaßnahmen nicht ausreichen. Dies muss jedoch stets eingegrenzt auf das konkrete Vorkommnis erfolgen und darf die IT-Sicherheit oder Persönlichkeitsrechte nicht über die konkrete Ermittlung hinausgehend schwächen.

Veränderung 5: Nachhaltige Digitalisierung

> *Digitalisierung trägt durch ihren Ressourcenverbrauch zur Klimakatastrophe bei – klug gestaltet könnte sie jedoch einen Beitrag zur Bekämpfung der Klimakrise leisten.*

Die Digitalisierung trägt in ihrer heutigen Form erheblich zur Beschleunigung des Klimawandels bei. Der Datenhunger wächst exponentiell und mit ihm der Ressourcen- und Energieverbrauch. Effizienzgewinne werden häufig durch Rebound-Effekte „aufgefressen“. Es fehlen Daten, Forschung sowie mehr gemeinsame Betrachtung von Digitalisierung und

Klimakrise, um die Klimawirkung der Digitalisierung besser zu kennen und signifikant zu reduzieren.
So verschlingt der Ausbau digitaler Infrastrukturen oft unnötige Ressourcen. Kupferbasierte Infrastruktur hat bei begrenzter Datenübertragungsrate einen relativ hohen Energieverbrauch. Sie wird zu langsam abgelöst, Glasfaser wird aus kommerziellen Interessen doppelt verlegt und Mobilfunknetze sogar drei- und vierfach ausgebaut, anstatt knappe Ressourcen effizienter gemeinschaftlich zu nutzen. Schlechte Reparierbarkeit verkürzt künstlich die Nutzungsdauer elektronischer Geräte, obwohl die längere Nutzung ein enormer Hebel zur Senkung des Ressourcenfußabdrucks ist. Energieeffizienz digitaler Geräte spielt bei ihrer Produktion eine zu geringe Rolle, das gilt erst recht bei der Entwicklung von Software. Es wird flächendeckend zu wenig repariert, nachgenutzt und recycelt, weil Neukauf oft billiger ist, denn Klimafolgen sind nicht eingepreist. Voreinstellungen von Anwendungen oder Nutzungsalgorithmen begünstigen höhere Datenmengen und längere Nutzung. Auch der Bund als sehr großer Einkäufer von IT bleibt bisher weit hinter Absichtserklärungen zurück, den Ressourcen-Fußabdruck zu senken.
Wir lehnen Aufrüstung und Waffenexporte auch bezogen auf Cyberwaffen, Kampfdrohnen und andere Technologien für digitalisierte Kriegsführung ab, denn Militär und Krieg sind maximal entfernt von sozialer und ökologischer Nachhaltigkeit und alles andere als geeignet für gemeinwohlorientierte Digitalisierung. Nachhaltige Sicherheit ist zivile Sicherheit.

Wir fordern:

- mehr **Transparenz** zur Klimawirkung und zum Ressourcenverbrauch der Digitalisierung,
- mehr **Forschung** zu und Förderung von klimafreundlicher und energieeffizienter Digitalisierung bei Rechenzentren, Software, Webdiensten, Netzen und Hardwareproduktion,
- **ressourcensparsamen Breitbandausbau**, z.B. durch Förderung von Open Access Netzen und ein Verbot von Glasfaser-Doppelverlegung bei vorhandenem Open Access Netz sowie durch regionales Roaming für Mobilfunk im ländlichen Raum,
- **Datensparsamkeit** als Methode zur Reduktion klimaschädlicher Effekte. Training und Einsatz von KI sowie von Blockchains gegen den erwarteten sozialökologischen Nutzen kritisch abzuwägen und soweit möglich und sinnvoll, energiesparsamere Methoden anwenden,
- die Einführung eines bundesweiten, herstellerfinanzierten **Reparatur**-Bonus und eine nachhaltige Förderung von Reparatur-Initiativen und -Kompetenzen, mehr Nachnutzung und Recycling elektronischer Geräte; ein Recht auf Reparatur und Verbot von Verträgen, die auf eine vorzeitige Neuanschaffung von IT-Geräten abzielen (zum Beispiel Handyverträge, bei denen alle zwei Jahre ein neues Endgerät im Vertrag enthalten ist),
- **Nachhaltigkeit bei öffentlicher IT**, mit klaren und ehrgeizigen Zielen und durch verbindliche Vorgaben beim Einkauf von IT-Produkten und Diensten. Benötigte Geräte wie Smartphones oder Laptops und deren Software müssen so beschaffen sein, dass sie möglichst lange genutzt und gut repariert und aktualisiert werden können, um die Kosten gering zu halten und die Umwelt zu schonen,
- **bewaffnete Drohnen** müssen völkerrechtlich bindend geächtet werden; keine Entwicklung oder gar Export von Cyberwaffen, stattdessen Investitionen in die zivile IT-Sicherheit.