Positionspapier der AG Digitale Agenda

Eine Digitale Agenda für alle

Mehr gesellschaftlicher Zusammenhalt. Mehr Miteinander und den Blick in die Zukunft. Die Chancen nutzen und die Risiken klein halten. Die Digitalpolitiker der SPD-Bundestagsfraktion fordern eine Fortschreibung der digitalen Agenda der Bundesregierung – mit klaren Zielen. Im Mittelpunkt: die Emanzipation und Selbstbestimmung der Menschen.

Unsere sozialdemokratische Idee von der digitalen Gesellschaft ist am Gemeinwohl orientiert, an Freiheit, Gerechtigkeit und Solidarität. Gerade in Zeiten des technologischen Wandels braucht es mehr gesellschaftlichen Zusammenhalt und ein neues Miteinander, wenn die Möglichkeiten breit genutzt und die Risiken kollektiv abgesichert werden sollen. Menschen sollen kompetent und selbstbestimmt an der digitalen Welt teilhaben. Dazu brauchen sie freien Zugang zu einem schnellen und sicheren Netz, starke Rechte als Bürger, als Verbraucher und Erwerbstätige sowie einen Anspruch auf gute Bildung, ein Leben lang.

Die digitale Technologie entwickelt sich rasend schnell, und es entstehen neue Chancen und Herausforderungen: Die weltweite Verfügbarkeit großer Datenmengen, explodierende Rechnerkapazitäten und Durchbrüche im maschinellen Lernen machen möglich, wovon bisher nur Science Fiction-Autoren träumten: Lernfähige Maschinen könnten immer mehr von dem übernehmen, wofür es bislang Menschen gebraucht hat. Nach der Automatisierungswelle in der Industrie, die uns viel schwere Arbeit abgenommen hat, geht es nun vor allem um die Automatisierung von Kopfarbeit. Doch wo bleibt dabei der Mensch?

Der Einsatz digitaler Technologien kann unterschiedlichen Zielen dienen. Bekanntermaßen ermöglichen sie neue Formen demokratischer Beteiligung ebenso wie Überwachung. Sie können als Instrument der Arbeitserleichterung oder Arbeitsverdichtung wirken. Roboter können menschliche Arbeit verdrängen. Assistenten bieten die Möglichkeit, die Ressourcen der wenigen Fachkräfte besser einzusetzen. Wie kann sichergestellt werden, dass digitale Technologien zum Wohl der Gesellschaft beitragen?

Mit der Fortschreibung der digitalen Agenda haben wir uns folgende Ziele gesetzt:

- Wir wollen den Menschen im digitalen Wandel die selbstbestimmte Teilhabe an Familienleben, Erwerbsarbeit und gesellschaftlichem Engagement eröffnen. Weiterbildung, rechtliche Rahmenbedingungen und eine verlässliche soziale Absicherung sollen gewährleisten, dass der digitale Wandel in Wirtschaft und Arbeit den Menschen nutzt.

- Wir wollen, dass durch den digitalen Wandel mehr Freiheit und keine neuen Diskriminierungen entstehen. Daten- und Verbraucherschutz sowie verlässliche IT-Sicherheit sind

wichtige Grundlagen für das Vertrauen und die Akzeptanz jeder weiteren Digitalisierung. Digitale Souveränität, sichere Infrastrukturen und digitale Produkte sind dafür ebenso unerlässlich wie starke und unabhängige Kontrollinstanzen.

- Wir wollen, dass die Menschen sich dem steten digitalen Wandel gewachsen fühlen, dass sie kompetent und souverän an der digitalen Welt teilhaben können. Gute und zeitgemäße Bildungsangebote in den Schulen, in beruflicher Aus- und Weiterbildung, an Hochschulen und in der Erwachsenenbildung müssen für alle Menschen offen zugänglich und auch als stete Begleitung im Erwerbsleben zu nutzen sein.

1. Digitale Wirtschaft und die Zukunft der Arbeit

Die Digitalisierung schafft neue Märkte und Geschäftsmodelle - sie ist eine Chance für unsere Zukunft. Wir müssen die Digitalisierung zum wirtschaftlichen Rückgrat unserer Zukunft werden lassen. Technologie und Fortschritt darf dabei aber kein Selbstzweck sein. Die Digitalisierung stellt Arbeitnehmer und Unternehmer vor immer neue Herausforderungen. Wir müssen heute schon dafür sorgen, dass die Arbeitsplätze von Morgen den Erwerbstätigen auch weiterhin Sicherheiten bieten. Dazu braucht es ein Recht auf stete Weiterbildung und die Möglichkeit, mobil zu arbeiten. Des Weiteren ist der Schutz von Beschäftigtendaten sicherzustellen, so dass Menschen in digitalisierten Arbeitsabläufen nicht zum gläsernen Objekt der Optimierung werden. Die neue Arbeitswelt 4.0 erfordert es, die beschäftigten Menschen in den Mittelpunkt zu stellen.

Die Programme müssen sich an unterschiedliche Arbeitsbereiche und –felder anpassen**:**

a. Die so genannte **Kopfarbeit**, wie sie von medizinischem, juristischem oder administrativ tätigem Fachpersonal ausgeübt wird, steht im Fokus des künftigen Automatisierungsschubes. Wenn Entscheidungen von Maschinen unterstützt oder teils übernommen werden sollen, muss eine souveräne Mensch-Maschine-Kommunikation gewährleistet werden. Daher gilt es, die stete Weiterbildung von Erwerbstätigen zu gewährleisten, die ihnen einen souveränen Umgang mit digitalen Medien und Methoden, algorithmischen Entscheidungssystemen, Big Data und Technologien Künstlicher Intelligenz erlaubt.

b. **Unterstützung von Digitalisierungsprozessen im Dienstleistungssektor** und bei **kleineren und mittlere Unternehmen**: Es gilt, Chancen und Herausforderungen im Bereich der Plattformökonomie regulativ Rechnung zu tragen – durch Weiterentwicklung der wettbewerbsbehördlichen Aufsicht und Missbrauchskontrolle. Dazu braucht es neuartige Maßnahmen zum Schutz und zur Förderung der Mitbestimmung der dort frei Beschäftigten. Digitalisierungsprozesse bei kleinen und mittleren Unternehmen sollen im Rahmen der Digital Hub Initiative darin unterstützt werden, Verwaltungsabläufe, Produktion und Distribution so umzugestalten, dass sie wettbewerbsfähig bleiben und die Beschäftigten die entsprechenden Kompetenzen aufbauen. Dazu brauchen wir wettbewerbsrechtliche sowie AGB-rechtliche Regulierungsoptionen.

c. **Industrielle Fertigung/ Arbeit in der Industrie 4.0:** Die Automatisierung der Industrie 4.0 ist gut vorangekommen. Hier sollen die Beschäftigten verstärkt in den Blick genommen werden, im Bereich der Weiterbildung für die Digitalisierung industrieller Produktion und der sozialen und rechtlichen Absicherung, v.a. im Bereich flexibler Arbeitszeitmodelle.

d. **Startup-Förderung:** Gründungen und Selbständigkeit stellen einen Schwerpunkt wirtschaftlicher und gesellschaftlicher Reorganisation dar. Daher müssen wir die Weiterbildung von **selbstständig Erwerbstätigen** (Selbständige, Gründer, Solo-Selbständige) fördern. Neben der Bereitstellung entsprechender Angebote können alternative Finanzierungskonzepte wie Stipendien die Qualifizierung begünstigen: sei es im Bereich der Entwicklung und Anwendung oder in der Weiterbildung und Beratung. Zudem gilt es, selbständig Erwerbstätige in die Systeme sozialer Absicherung einzubeziehen.

e. **Mitarbeiterbeteiligung:** Hier müssen richtige Formen gefunden werden, allen Mitarbeiter – und nicht nur der Führungsebene – die Möglichkeit zu geben, sich am Unternehmen zu beteiligen. Durch die Gewährung von staatlichen Zuschüssen und Steuervergünstigungen gilt es, Anreize zu schaffen.

Menschen, die keine Erwerbsarbeit haben und die, deren Arbeit sich ändert, brauchen unsere Unterstützung! Wir müssen sie dabei unterstützen, sich auf den digitalen Wandel und den technologischen Fortschritt einzulassen und in ihm zu bestehen. Dazu benötigen sie eine verlässliche soziale Absicherung sowie zielgenaue Beratungs- und Weiterbildungsangebote der Arbeitsagentur, die auch ihre persönliche Lebenssituation berücksichtigt. Das **Chancenkonto** bietet Weiterbildungsoptionen für alle Gruppen.

Was im Kleinen nicht funktioniert, kann im Großen nicht gut werden – daher beginnt gute Arbeit bei den Menschen und den Arbeitgebern. Dabei verlieren wir den internationalen Wettbewerb nicht aus den Augen. Damit das gelingt, brauchen die vielen Marktteilnehmer Orientierung - nach dem Grundsatz: Gleiches Geschäft, gleiche Risiken, gleiche Regeln.

Unnötige Wettbewerbsnachteile, Rechtskomplikationen und Regulierungskosten sind zu vermeiden. Dabei verwehren wir uns gegen die Diffamierung von Datenschutz-, Verbraucherschutz- und Umweltschutzregelungen als Wettbewerbsnachteil. Die EU muss durch Vollendung des EU-Binnenmarktes beispielgebend vorangehen. Wir brauchen einen fair ausgestalteten Wettbewerb – und zwar nachhaltig. Klassische Steuerungsinstrumente wie die Steuerpolitik, das Kartell-, Fusions- und Wettbewerbsrecht müssen weiterentwickelt und mit neuen Anreizsystemen kombiniert werden (Gaming). Ziel ist es, ein **Level-Playing-Field** in allen Bereichen zu schaffen.

Zur Aufrechterhaltung staatlicher Handlungsfähigkeit braucht es eine Steuerreform. Sie beginnt bei der Verpflichtung internationaler Online-Händler zur Abführung inländisch anfallender Umsatzsteuer und umfasst auch die faire Besteuerung der global operierenden Internetunternehmen für in Europa erwirtschaftete Gewinnen.

2. Bildung, Lehre und Forschung in einer digitalen Welt

Die notwendigen Veränderungen des Bildungssystems durch den digitalen Wandel wurden im Koalitionsvertrag für alle Bereiche verankert. Sie ermöglichen, dass in der gesamten Bildungskette Kompetenzen für die digitale Welt erworben und erneuert werden können.

a. **Digitalpakt**: Kernbestandteil für den digitalen Wandel in Schulen ist der Digitalpakt. Mit einer Investition von fünf Milliarden Euro wollen wir die digitale Ausstattung in allen **Schulen** verbessern und damit die Bildung in der digitalen Welt unterstützen. Von der Bundesregierung und den Landesregierungen erwarten wir ein Konzept, wie diese digitale Ausstattung dann nachhaltig auf einem aktuellen Stand gehalten werden kann. Mit der Entwicklung einer offenen Bildungsplattform unterstützen wir Lehrkräfte und Schüler sowie externen Bildungsinteressierte. Das schließt die Nutzung von offen lizenzierten Lernmaterialien (OER) ein. Weitere Maßnahmen sind etwa regionale Kompetenzzentren und zeitgemäß ausgestattete Lernwerkstätten für **verschiedene Zielgruppen**. Der Hochschulbereich beinhaltet die Vermittlung von Grundlagen der Datenanalyse und Programmierung sowie neuartige Zertifikate beruflicher Weiterbildung.

b. Forschung: Die Forschung soll in den Bereichen Mikroprozessortechnik, IT-Sicherheit, künstliche Intelligenz, Data Science, Digital Humanities, Blockchain-Technologie, Robotik und Quanten-Computing besonders gefördert werden. Dazu muss die Finanzierung verbessert werden - durch mind. 3,5% des BIP bis 2025**.**

c. **Aufhebung des Kooperationsverbotes:** Eine **rechtliche Voraussetzung** für den Erfolg dieser Initiative besteht in der Aufhebung des Kooperationsverbotes in der Bildungspolitik. Weiterhin muss eine Regelung von Bildungs- und Wissenschaftsschranken im Urheberrecht gefunden werden. Die Datenzugriffs- und Nutzungsrechte für außeruniversitäre Bildungs- und Forschungsinstitutionen sowie zivilgesellschaftliche Akteure werden geklärt.

d. **Aufbau eines Multi-Gigabit-Netzes** für wissenschaftliche Einrichtungen: Einige wissenschaftliche Einrichtungen, z.B. in der Physik, sind auf die Verarbeitung sehr großer Datenmengen angewiesen. Sie müssen – im Rahmen des allgemeinen Ausbaus des Breitband-Internets – Multi-Gigabit-Anschlüsse erhalten.

3. Digitale Infrastruktur

Flächendeckende Hochgeschwindigkeitsnetze sind die zentrale Voraussetzung einer digitalen Gesellschaft. Der Ausbau dieser Netze kommt jedoch weder im Festnetzbereich noch im Mobilfunk mit der erforderlichen Geschwindigkeit voran. Damit das im Koalitionsvertrag formulierte Ziel, allen Menschen in Deutschland bis 2025 einen flächendeckenden Gigabit-Anschluss zu bieten, realisiert werden kann, sind verstärkte Anstrengungen notwendig:

f. **Glasfaser:** Die bisherige Förderung ist konsequent ausschließlich auf Glasfaser neu auszurichten. Für bisher geförderte Ausbaugebiete sind Aufrüstungsmöglichkeiten auf den Gigabitstandard zu entwickeln. Die Erstellung der Förderkulisse für das Gigabit-Netz

ist mit Hochdruck voranzutreiben und zu notifizieren. Die Aufgreifschwelle ist hochzusetzen.

g. **WLAN / Freifunk:** Die Einrichtung **von WLAN-Hotspots in** öffentlichen Einrichtungen und Freifunk wird gefördert. Die Gemeinnützigkeit von Freifunk ist anzuerkennen.

h. **5. Mobilfunkgeneration (5G):** Eine digitale Gesellschaft benötigt neben Hochleistungsglasfasernetzen auch den Ausbau **flächendeckender Gigabitnetze im Mobilfunk**. Die Versteigerung der Frequenzen 5G wird derzeit vorbereitet. Im Rahmen der Versorgungsauflagen muss der Grad der Flächenabdeckung mindestens den Standard der LTE-Ausbauauflagen erfüllen und darüberhinausgehend alle Verkehrswege einschließen. Zur Versorgung von nicht eigenwirtschaftlich erschließbaren Regionen wird das nationale Roaming ermöglicht, eine unter Umständen notwendige Verpflichtung der Mobilfunkbetreiber insbesondere in ländlichen Räumen muss geprüft werden. Die Frequenzvergabe wird an eine Staffel konkreter Ausbauzwischenziele für den Ausbau der 5G-Netze gekoppelt, die bei Nichterfüllung wirksame Sanktionsmechanismen in Kraft setzen können. Perspektivisch sind langfristig die Zeiträume für die Vergabe niedriger Frequenzbereiche anzugleichen, um deren effektive Ausnutzung durch Mobilfunkangebote zu ermöglichen.

Unter dem Stichwort **Next Generation Networks** werden neuartige Netzinfrastrukturen diskutiert, bei denen Datenanalysekapazitäten in den Netzen integriert sind. Deren Nutzen, Risiken und ggf. Kompatibilität mit dem bereits geplanten Infrastrukturausbau ist zu prüfen.

4. Datenschutz, Verbraucherschutz, IT-Sicherheit und Vertrauen

Datenschutz schützt keine Daten, er dient der Selbstbestimmung und der Privatsphäre in der digitalen Welt. Mit der **EU-Datenschutz-Grundverordnung** wurde eine Harmonisierung der Regeln zur Nutzung personenbezogener Daten erreicht, die nun durch die **E-Privacy-Verordnung** zu ergänzen sind. Sie regelt die Nutzung solcher Daten, die sich aus dem Kommunikationsverhalten von Menschen ergeben. Die Normen sind zu implementieren und gesetzgeberisch zu begleiten. Die Sicherheit der Datenkommunikation steht mit der Vernetzung vor immer größeren Herausforderungen. Sicherheitspolitik beginnt bei der Analyse neuer Sicherheitsrisiken und der Weiterentwicklung von Lösungsansätzen.

a. **Bundesbeauftragte für den Datenschutz und die Informationsfreiheit stärken:**

- Zur Erfüllung der Aufgaben erhält die BfDI über die in den Haushaltsplänen 2018 und 2019 vorgesehenen Stellen hinaus einen weiteren personellen Aufwuchs
- Der Service- und Beratungsbereich bei der BfDI wird ausgebaut
- Der Jahresbericht der BfDI wird ab 2019 im Plenum des Deutschen Bundestages vorgestellt und anschließend nach Debatte in die Ausschüsse verwiesen

b. **Ausbau des Bundesamt für Informationssicherheit** (BSI),

- als neutraler Wächter (Meldestelle für Sicherheitslücken) und Koordinator lokaler, nationaler, europäischer und internationaler Sicherheitsmechanismen.

- als unabhängiger Berater von Unternehmen und Institutionen in der IT-Sicherheit.
- als Inkubator und Aufsichtsbehörde für Standard-Entwicklung und Zertifizierung von sicheren digitalen Produkten und Dienstleistungen (Security-by-Design).

  Kompetenzen und personellen Ressourcen sind deutlich auszubauen und durch eine unabhängige Fachaufsicht zu begleiten.

c. **Fortschreibung der IT-Sicherheitsgesetzgebung**: Gesetzliche Rahmenbedingungen müssen durch Fortschreibung der IT-Sicherheitsgesetzgebung vorangebracht werden. Sie umfassen Regeln zur Produkthaftung sowie der Entwicklung und Etablierung von Gütesiegeln. Anwendungsfelder und Risiken durch Bots sind zu untersuchen, orientiert an Möglichkeiten ihrer Identifikation und Kennzeichnung.

d. **Produkthaftung**: Ein zentrales Sicherheitsinstrument sind Regelungen für die Produkthaftung in der digitalen Welt, die unter Berücksichtigung der unterschiedlichen Entwicklungs- und Evaluationsmechanismen von Software fortzuentwickeln ist.

e. **Stakeholder**: Der Umgang mit aktuellen Sicherheitsrisiken erfordert eine Zusammenarbeit aller Akteure – in einer Art und Weise, die demokratisch legitimierten Institutionen Einsicht und Kontrolle erlaubt. Der Nationale Pakt Cybersicherheit und die Bund-Länder-Kooperation sind fortzuentwickeln. Forschungsförderung und die Ausbildung von IT-Sicherheits-Fachkräften haben oberste Priorität. Sicherheitsrelevante Schlüsseltechnologien sind, durch einen Fonds des Bundes vor dem Ausverkauf zu schützen.

f. **IT-Sicherheit:** Die Geheimhaltung und Nutzung von IT-Sicherheitslücken durch den Staat, sei es für den Einsatz von Staatstrojanern für die Quellen-TKÜ, für die Online-Durchsuchung oder gar für digitale Abwehrschläge **(Hack Backs)** ist mit der Förderung der allgemeinen IT-Sicherheit nicht zu vereinbaren. Wir werden uns dafür einsetzen, dass der Staat den Herstellern IT-Sicherheitslücken jederzeit bekanntmacht, so dass diese geschlossen werden können. Wichtiger als die von den Diensten losgetretene Diskussion über proaktive Cyberabwehr, die vor allem eine Vielzahl verfassungs-, völker-, und kriegsrechtlicher Probleme aufwirft, ist es, die eigenen Systeme zu sichern, robuster zu machen und vor Cyberangriffen zu schützen.

5. Der digitale Staat

Die Digitalisierung von Verwaltungsprozessen und die Automatisierung von Standardprozessen sind wesentliche Bausteine für die Sicherung staatlicher Handlungsfähigkeit und die Gewährleistung moderner staatlicher Dienstleistungen in einer vernetzten Welt. Der Staat muss sich als Wegbereiter des digitalen Wandels begreifen: Durch eine ausgewogene Technologiebeschaffung kann er in Fragen des Wettbewerbs und der Sicherheit Standards setzen. Dabei muss er Entwicklung und Verbreitung von Open Source Software unterstützen. Diesem Bereich kommt in den folgenden Jahren eine bedeutende Rolle zu.

a. **E-Government:** Das Ziel von E-Government ist die einfache und nutzerfreundliche Gewährleistung öffentlicher Güter und Dienstleistungen jenseits von Öffnungszeiten und

starren Terminen. Dazu braucht es die Digitalisierung über Verwaltungsportale im Verbund, wie sie im Online-Zugangsgesetz vereinbart ist. Projekte der öffentlichen Verwaltung müssen Mittel für interne Schulung, Evaluation und Weiterentwicklung vorsehen. Die Einrichtung einer E-Government-Agentur dient der Entwicklung von einheitlichen Standards. Bürgerkontos sollen Transparenz und Kontrolle über die Verarbeitung personenbezogener Daten herstellen. Distributed Ledger Technologien (Blockchain) sind eine Möglichkeit, transparente und sichere E-Government-Prozesse zu erproben.

b. **Umsetzungsmaßnahmen:** Dazu gehören die weitgehende Abschaffung die Schriftformerfordernisse, die Prüfung von Normen und Registern auf Standardisierungsfähigkeit, die Einführung der elektronischen Identifizierung und E-Akte sowie eine verschlüsselte Kommunikation via PGP und/oder SMIME.

c. **Open Data Strategie:** Die Realisierung der Open Data Strategie braucht die Bereitstellung von Umsetzungsmitteln für alle deutschen Behörden. Der Verfügbarkeit öffentlicher Daten kommt eine wesentliche Rolle in der Entwicklung und Erprobung nationaler KI-Technologien zu (inkl. der Standardentwicklung). Das Informationsfreiheitsrecht ist zu einem umfassenden Transparenzrecht fortzuentwickeln.

d. **Open Government Partnership**: Wir brauchen transparente Prozesse in Regierung und Verwaltung. Die Beteiligung der Bevölkerung an der Entwicklung neuer gesetzlicher Vorhaben ist ein wesentlicher Baustein für einen modernen Staat im digitalen Zeitalter. Die Umsetzung und Weiterentwicklung nationaler Aktionspläne im Rahmen der Open Government Partnership ist deshalb mit den notwendigen Mitteln auszustatten

6. Algorithmen und Künstliche Intelligenz

Die Entwicklung Künstlicher Intelligenz stellt neue Herausforderungen an die **Datenpolitik**: Denn einerseits bestimmt sie, auf Basis welcher Daten KI-Technologien entwickelt, angewandt und geprüft werden dürfen. Andererseits braucht eine verantwortungsvolle Entwicklung von KI-Technologien das „richtige Futter“: repräsentative, aktuelle Daten, die dem jeweiligen Zweck entsprechen.

a. **Schutz und Regulierung:** Es ist ein rechtlicher Rahmen zu schaffen, der die Souveränität im Umgang mit Daten garantiert. Das erforderliche Schutzniveau und die notwendige Regulierung bestimmen sich aus der Datenart - so muss es beispielsweise bei Verkehrsdaten, Maschinendaten oder Geodaten darum gehen, neue Datencontainer sowie Datenmonopole zu verhindern. Bei personenbezogenen Daten muss das Recht auf informationelle Selbstbestimmung gesichert werden. Daten, die sich aus dem Kommunikationsverhalten von Menschen ergeben, brauchen eine gesonderte Regulierung (E-Privacy-Verordnung). Die Analyse von Metadaten, Kommunikationsinhalten und -verhalten ermöglicht weitreichende Analysen individueller Charakterzüge und Verhaltensprognosen. Alle Bürger müssen Opt-Out-Optionen erhalten. Neben einer klugen Regulierung von Datenzugangsrechten braucht es die Entwicklung von Technologien, die die Qualität

von Datensets sichern. Blockchain-Technologien bieten hier eine Lösung, die weiter zu erproben und zu prüfen ist.

b. **Demokratische Kontrolle:** Algorithmische Entscheidungssysteme und KI-Technologien brauchen demokratische Kontrolle. Entscheidungen darüber dürfen nicht allein Unternehmen überlassen werden. Die Funktionsweise algorithmischer Entscheidungssysteme muss durch demokratisch legitimierte Akteure einsehbar und überprüfbar sein, die bei Bedarf eingreifen können. Eine Aufsichtsbehörde sollte einen Überblick über die Entwicklung haben und bei Bedarf Missbrauchskontrollen durchführen sowie beraten können. Dazu braucht es den Aufbau von Kompetenzen und Ressourcen im Bereich Algorithmen-Auditing sowie einen Rechtsrahmen, der den legitimen Zugang zu Datensets absichert. Es darf keine Diskriminierung von Einzelnen oder Gruppen als Folge von KI entstehen.

c. **Menschliche Intervention**: Zur Gewährleistung menschlicher Entscheidungshoheit muss die **Kommunikation von Mensch und Maschine** optimiert werden. Das bedeutet, Mensch-Maschine-Schnittstellen zu entwickeln, welche die Varianz algorithmischer Entscheidungen sichtbar machen (z.B. Therapiemöglichkeiten bei Krebspatienten) und effektive Intervention in allen Sektoren zu erlauben. Die Förderung von Forschung und Kooperationen zwischen betroffenen Stakeholdern sind dazu unerlässlich.

d. **Kauf-, Vertrags- und Haftungsrecht für KI weiterentwickeln:** Damit die Haftungslage bei Mensch-Maschine-Interaktion bzw. Assistenzsystemen geklärt ist und Maschinen mit Maschinen bindende Verträge aushandeln können, müssen die entsprechenden Rechtsbereiche weiterentwickelt werden.

7. Bedeutung der europäischen und internationalen Ebene für die Digitalpolitik

Unter Berücksichtigung des technischen Wandels gelten universelle Spielregeln wie zentrale **Freiheits- und Schutzrechte** auch in der digitalen Welt. Die europäische digitale Grundrechtecharta war ein Anfang! Die Wirksamkeit von Grundrechten gegenüber Unternehmen gewinnt durch die wachsende Bedeutung privater Plattformen an Relevanz. Der Ansatz soll zu einem digitalen Völkerrecht fortentwickelt werden (UN Charta Digitalisierung). So können Chancen und Risiken der Digitalisierung zu einem Ausgleich gebracht werden.

Mit der wachsenden Bedeutung des Internets und der wachsenden Abhängigkeit von vernetzter Technik wird die Frage nach Sicherheit im Netz immer wichtiger. Der NSA-Skandal und die Internetkriminalität verunsichern die Menschen – zu Recht.

Daher braucht es eine neuartige **Balance**, die das Freiheitsversprechen des Netzes fortführt und realen Sicherheitsrisiken begegnet. Es gilt also einerseits, die freiheitliche und offene Architektur zu erhalten, sich Angriffen auf die Netzneutralität ebenso entgegen zu stellen wie der Verpflichtung auf Upload-Filter. Andererseits muss aus vermeintlicher Sicherheitspolitik - dem anlasslosen, umfassenden Ausspähen privater und öffentlicher Kommunikation - eine echte Sicherheitspolitik werden, die die Grundbedürfnisse der Menschen schützt. Cy-

berangriffen muss durch hohe Standards im Bereich Datenschutz und der IT-Sicherheit vorgebeugt werden. Deutschland ist in diesem Bereich zu einem führenden Standort auszubauen.

Neuen Risiken, die sich aus der Entwicklung von Technologien Künstlicher Intelligenz ergeben, ist ebenfalls zu begegnen. Auf nationaler Ebene braucht es eine zeitnahe Übersicht über den Stand der technologischen Entwicklung, auf Basis derer eine adäquate Risiko-Analyse erfolgen kann. Zu berücksichtigen ist der politökonomische Entwicklungs- und Anwendungskontext von KI-Technologien, die Interaktion von Systemen (Plattformen) und deren Zusammenspiel mit Trends im Bereich informationeller, automatisierter oder auf kritische Infrastrukturen ausgerichteter Kriegsführung. In einem internationalen Kontext, der etwa durch zentrale Datenakkumulations- und Steuerungskapazitäten in den USA und dezentrale Angriffsinstrumente in Russland bestimmt wird, ist Sicherheit ohne internationale Kooperation undenkbar. Globale Sicherheitspolitik muss klare Regeln und Abkommen im Blick haben und neu ausgerichtet werden: Die knappen technischen Ressourcen und Kompetenzen dürfen nicht weiter zu einem sicherheitspolitischen Wettrüsten eingesetzt werden, sondern zur Reduzierung realer Risiken - zur effizienten Bereitstellung elementarer Güter und Dienstleistungen für die Gesamtheit der Menschen. Wir brauchen eine werte-orientierte Sicherheitspolitik, die global Anreize bietet, die informationelle Kriegführung zu überwinden und wir brauchen internationale Vereinbarungen zur Ächtung und Abrüstung von unverantwortbaren digitalen Angriffsszenarien.

8. Organisation der Digitalpolitik und Zusammenspiel von Regierung und Parlament

Um die politische Gestaltung des digitalen Wandels voran zu bringen, braucht es die **strategische und zukunftsorientierte Definition einer digitalen Agenda der Bundesregierung und die effektive Koordinierung ihrer Umsetzung** durch das Digitalkabinett. Diese muss die verschiedenen Zusammenhänge zwischen unterschiedlichen Politikfeldern berücksichtigen.

Der Arbeit des Digitalkabinetts wollen wir eine frühzeitige, enge und kritische **parlamentarische Begleitung** an die Seite stellen. Der Ausschuss Digitale Agenda soll für die parlamentarische Begleitung die Koordinierung und Federführung für die Planung, Steuerung, Vorbereitung und Durchführung der digitalpolitischen Vorhaben bekommen und zudem ein entsprechendes Monitoring der Umsetzung der Digitalisierungsstrategie durchführen.