Positionspapier der AG Inneres und der AG Digitale Agenda

„Vertrauen und Sicherheit im digitalen Zeitalter“

Zentrale Botschaften:

- SPD will, dass digitaler Wandel zu sozialem Fortschritt wird, am Gemeinwohl orientiert und mit gerechte Teilhabe für alle Menschen. Dafür brauchen die Bürgerinnen und Bürger Souveränität, Freiräume und Sicherheit im digitalen Raum.
- Politik und Verwaltung haben die Chance, durch Digitalisierung und Transparenz neues Vertrauen zu schaffen. Dabei müssen der Schutz der Bürgerrechte, Privatheit und Datensicherheit gewährleistet sein.
- Wenn Politik und Verwaltung digital werden, Wirtschaft und Arbeit, Bildung und Zivilgesellschaft, dann wird IT zunehmend Grundlage allen öffentlichen und gesellschaftlichen Lebens. Damit wird die Integrität und Sicherheit digitaler Strukturen zur staatlichen Aufgabe.

Im Fokus: Vertrauen und Sicherheit im digitalen Zeitalter

Unsere sozialdemokratische Idee vom digitalen Wandel ist es, ihn zum Fortschritt für Mensch und Gesellschaft zu entwickeln, eine Gesellschaft, die am Gemeinwohl orientiert ist, an Freiheit, Gerechtigkeit und Solidarität. Es ist unsere Verantwortung, allen Menschen gleichermaßen Zugang zum digitalen Wandel als sozialen Fortschritt zu eröffnen und dabei neue wie alte Unfreiheiten, Ungleichheiten und Diskriminierungen zu verhindern.

Besondere Chancen liegen in der Digitalisierung für ein effizientes, transparentes und bürgernahes Handeln von Politik und Verwaltung und damit für eine Stärkung des Vertrauens in die staatliche Handlungsfähigkeit. Damit Menschen sich mit Vertrauen und Zuversicht auf diesen Wandel einlassen können, brauchen sie Freiräume und Souveränität, aber eben auch Sicherheit: Durch starke Bürger- und Verbraucherrechte, starke Kontrollinstanzen und den Schutz von Privatsphäre und persönlichen Daten einerseits, sowie die Bewältigung von neuen Sicherheitsrisiken – etwa im Bereich kritischer Infrastrukturen und der Informationssicherheit – andererseits. Wenn Politik und Verwaltung digital werden, Wirtschaft und Arbeit, Bildung und Zivilgesellschaft, dann wird IT zunehmend Grundlage allen öffentlichen und gesellschaftlichen Lebens. Damit wird die Integrität und Sicherheit digitaler Strukturen zur staatlichen Aufgabe.

Digitale Infrastrukturen ebenso wie Produkte und Dienstleistungen brauchen eine resiliente IT/Cybersicherheit, damit die digitale Gesellschaft ein Ort der Freiheit, der offenen Kommunikation, der gesellschaftlichen Teilhabe und der individuellen und unternehmerischen Selbstentfaltung sein und bleiben kann. Zudem muss der Staat, so gibt es das Bundesverfassungsgericht vor, seine Eingriffsrechte in der Gesamtschau der Überwachung stets mit den Freiheitsrechten der Bürger in Einklang halten.

Die AG Innen der SPD-Bundestagsfraktion setzt in der Digitalpolitik daher folgende Schwerpunkte:

I. Politik und Verwaltung - digital und offen

Das Grundvertrauen der Bürger in den Staat ist Basis für Demokratie und Rechtsstaat und damit ein hohes Gut, das es zu wahren und immer wieder zu erneuern gilt. In der Digitalisierung von

Politik und Verwaltung (eGovernment, openData, openGovernment) liegt die Chance, das Vertrauen in die staatliche Handlungsfähigkeit (wieder) zu stärken, Prozesse offener und effizienter zu gestalten und dabei nahe am Bürger zu agieren.

1. Die konsequent durchgängige Entwicklung digital gestützter und am Nutzer orientierter Prozesse und Dienstleistungen der Verwaltung
2. Die konsequente Offenlegung von Prozessen und Daten der Verwaltung und die Entwicklung neuer Formen digitaler Mitbestimmung, Regierungskontrolle und digitaler Souveränität
3. Die Entwicklung und Erprobung algorithmischer Entscheidungssysteme im Bereich der Verwaltung / Daseinsvorsorge (kontrolliert / evaluiert)

II. Bürgerrechte, Datenschutz und Privatheit

Damit die Menschen als Bürger und Verbraucher, im privaten wie im öffentlichen Leben in digitale Anwendungen vertrauen können, müssen sie auf die Unverletzlichkeit ihrer Privatsphäre, den Schutz ihrer persönlichen Daten und damit in die Integrität ihrer Daten- und Kommunikationssysteme vertrauen können.

1. Die vom Bundesverfassungsgericht angemahnte Gesamtschau der Überwachung beachten bei der Bewertung und Weiterentwicklung staatlicher Eingriffsrechte.
2. Personenbezogene Daten und private Kommunikation verdienen besonderen Schutz. Die unabhängigen Datenschutz-Aufsichtsbehörden in Bund und den Ländern müssen besser ausgestattet werden, damit sie entsprechend ihrer Aufgaben zu den Regeln und Methoden für Datenschutz und Privatheit informieren und beraten können und Datenschutzverstöße konsequent geahndet bzw. abgestellt werden.
3. Die Förderung und den Einsatz sicherer und Ende-zu-Ende-verschlüsselter Kommunikation in allen sensiblen Bereichen

III. Integrität und Sicherheit von Daten und Infrastrukturen (IT-Sicherheit)

Weil die Integrität und Sicherheit digitaler Strukturen, Technologien und Produkte zunehmend Grundlage allen öffentlichen und gesellschaftlichen Lebens ist, sehen wir die IT-Sicherheit als staatliche Aufgabe und Verantwortung. Wir lehnen die Entwicklung und den Einsatz von Cyber-Angriffswerkzeugen und die Offenhaltung und Nutzung von IT-Sicherheitslücken durch den Staat ab, weil sie die allgemeine IT-Sicherheit beschädigen, und plädieren für eine strikt defensive Ausrichtung der Cyber-Sicherheitsstrategie.

1) Ausbau und Stärkung des BSI als unabhängiger Berater und Dienstleister in allen Fragen der Sicherheit in der Informationstechnik
2) Entwicklung von Gütesiegeln und Produkthaftungsregeln für digitale Produkte und Dienstleistungen, Verpflichtung zu Bekanntgabe und zeitnahem Beheben bekannter Sicherheitslücken
3) Vernetzung der Kompetenzen bei der Analyse von Sicherheitsvorfällen und -risiken und der Entwicklung von Lösungsoptionen
4) Forschung und Entwicklung für sichere, verschlüsselte Kommunikation und innovative Sicherheitstechnik unter Berücksichtigung der besonderen Chancen von Open Source

5) Aus- und Weiterbildung von Fachkräften für die IT-Sicherheit
6) Stete Weiterentwicklung der Sicherheit und Resilienz kritischer Infrastrukturen
7) Strikt defensive Ausrichtung der deutschen Cyber-Sicherheitsstrategie, keine Offenhaltung und Nutzung von Sicherheitslücken durch den Staat
8) Weltweite Ächtung staatlicher Cyberangriffe