Antrag 229/I/2025
Jusos LDK
Der Landesparteitag möge beschließen:

Für eine faschismusssichere Digitalpolitik

Wir schließen uns den 12 Forderungen von 29 digitalpolitischen Initiativen und Organisationen an die nächste Bundesregierung an. Die Forderungen wurden unter anderem vom Chaos Computer Club (CCC), dem D64 e.V., Pro Asyl e.V., Amnesty International, digitalcourage e.V., Digitale Gesellschaft e.V. und der Open Knowledge Foundation Deutschland unterzeichnet:

Wir fordern die neue Bundesregierung auf, eine digitale Brandmauer gegen den Faschismus zu errichten. Diese digitale Brandmauer muss Missbrauchspotentiale minimieren, Menschen und gesellschaftliche Gruppen ermächtigen sowie Menschenrechte und demokratische Werte, insbesondere Freiheit, Gleichheit und Solidarität, schützen und fördern. Die aktuellen Geschehnisse in den USA zeigen auf, wie Datensammlungen und -analyse genutzt werden können, um einen Staat handstreichartig zu übernehmen, seine Strukturen nachhaltig zu beschädigen, Widerstand zu unterbinden und marginalisierte Gruppen zu verfolgen.

Bekenntnis gegen Überwachung
Es ist ein Irrglaube, dass zunehmende Überwachung einen Zugewinn an Sicherheit darstellt. Sicherheit erfordert auch, dass Menschen anonym und vertraulich kommunizieren können und ihre Privatsphäre geschützt wird. Zu oft werden aktionistische Vorschläge wie die Chatkontrolle, Vorratsdatenspeicherung oder biometrische Überwachung als technische Allheilmittel für komplexe gesellschaftliche Herausforderungen präsentiert – ohne ihre massiven Missbrauchspotenziale zu berücksichtigen. Stattdessen braucht es eine evidenzbasierte Politik, die differenzierte Lösungsansätze ohne Massenüberwachung verfolgt. Es ist die Aufgabe des Staates, Grundrechte zu schützen. Dazu gehört insbesondere auch, den Missbrauch von Maßnahmen, Befugnissen und Infrastrukturen zu verhindern, heute und in Zukunft.

Schutz und Sicherheit für alle
IT-Angriffe wie die durch „Salt Typhoon“ zeigen die Gefahren staatlicher Hintertüren und unterstreichen: Die Stärkung von IT-Sicherheit und Ende-zu-Ende-verschlüsselter Kommunikation ist eine Frage gesamtgesellschaftlicher Resilienz. Gleichzeitig steht unabhängige und zivilgesellschaftliche Sicherheitsforschung, die Sicherheitslücken zum Wohle der Gesellschaft aufdeckt, immer noch unter Generalverdacht und wird kriminalisiert. Sicherheitslücken in Software müssen von allen staatlichen Stellen

Empfehlung der Antragskommission
Annahme in Fassung AK. Überweisung LG in BT (Konsens)

Der Landesparteitag möge beschließen:

Für eine faschismusssichere Digitalpolitik

Wir fordern die neue Bundesregierung auf, eine digitale Brandmauer gegen den Faschismus zu errichten. Diese digitale Brandmauer muss Missbrauchspotentiale minimieren, Menschen und gesellschaftliche Gruppen ermächtigen sowie Menschenrechte und demokratische Werte, insbesondere Freiheit, Gleichheit und Solidarität, schützen und fördern. Die aktuellen Geschehnisse in den USA zeigen auf, wie Datensammlungen und -analyse genutzt werden können, um einen Staat handstreichartig zu übernehmen, seine Strukturen nachhaltig zu beschädigen,Widerstand zu unterbinden und marginalisierte Gruppen zu verfolgen.

Wir schließen uns daher den 12 Forderungen von 29 digitalpolitischen Initiativen und Organisationen an die nächste Bundesregierung an. Die Forderungen wurden unter anderem vom Chaos Computer Club (CCC), dem D64 e.V., Pro Asyl e.V., Amnesty International, digitalcourage e.V., Digitale Gesellschaft e.V. und der Open Knowledge Foundation Deutschland unterzeichnet.

Wir fordern daher:

- Die biometrische Massenüberwachung des öffentlichen Raums sowie die ungezielte biometrische Auswertung des Internets wird verboten. Insbesondere wird aktiv gegen jede Form von Datenbank vorgegangen, die ungezielt Bilder, Videos und Audiodateien aus dem Internet nach biometrischen Merkmalen auswertet. Die entsprechenden Befugnisse des Bundesamts für Migration und Flüchtlinge werden zurückgenommen.
- Anlasslose und massenhafte Vorratsdatenspeicherung wird abgelehnt. Stattdessen werden grundrechtsschonende und effektivere Maßnahmen der Strafverfolgung wie das Quick-Freeze-Verfahren und die Login-Falle verfolgt.
- Eine automatisierte Datenanalyse der Informationsbestände der Strafverfolgungsbehörden sowie jede Form von Predictive Policing oder automatisiertes Profiling von Menschen wird abgelehnt. Die Kooperationen deutscher und USGeheimdienste werden eingeschränkt, insbesondere wird jede Art von automatisiertem Massenaustausch von

im Rahmen eines Schwachstellenmanagements konsequent an die Hersteller zur Behebung gemeldet werden. Sicherheit und Schutz dürfen dabei keine Frage von Privilegien sein, sondern müssen für alle Menschen gelten, insbesondere für marginalisierte Menschen und Gruppen.

Demokratie im digitalen Raum

Private Überwachung und Machtkonzentration müssen bekämpft werden. Die willkürliche und antidemokratische Machtausübung der Tech-Oligarchen um Präsident Trump erfordert einen Paradigmenwechsel in der deutschen Digitalpolitik und ein erneuertes Bekenntnis zu dezentralen öffentlichen Räumen sowie der konsequenten Rechtsdurchsetzung durch föderale Aufsichtsstrukturen. Gesunde digitale Räume leben auch von einer resilienten Gesellschaft mit starken digitalen Kompetenzen und einem demokratischen Diskurs, in dem digitale Gewalt keinen Platz hat. Dazu fordern wir ein Gewaltschutzgesetz, das seinen Namen verdient, einen Ausbau der digitalen Bildung und die Förderung des digitalen Ehrenamts.

Wir fordern daher:

- Die biometrische Massenüberwachung des öffentlichen Raums sowie die ungezielte biometrische Auswertung des Internets wird verboten. Insbesondere wird aktiv gegen jede Form von Datenbank vorgegangen, die ungezielt Bilder, Videos und Audiodateien aus dem Internet nach biometrischen Merkmalen auswertet. Die entsprechenden Befugnisse des Bundesamts für Migration und Flüchtlinge werden zurückgenommen.
- Anlasslose und massenhafte Vorratsdatenspeicherung wird abgelehnt. Stattdessen werden grundrechtsschonende und effektivere Maßnahmen der Strafverfolgung wie das Quick-Freeze-Verfahren und die Login-Falle verfolgt.
- Eine automatisierte Datenanalyse der Informationsbestände der Strafverfolgungsbehörden sowie jede Form von Predictive Policing oder automatisiertes Profiling von Menschen wird abgelehnt. Die Kooperationen deutscher und US-Geheimdienste werden eingeschränkt, insbesondere wird jede Art von automatisiertem Massenaustausch von Inhalts- oder Metadaten unterbunden.
- Die Überwachungsgesamtrechnung wird veröffentlicht, kontinuierlich fortgesetzt und der Umfang staatlicher Überwachungsbefugnisse dementsprechend gesetzgeberisch angepasst.
- Es wird ein Recht auf Verschlüsselung eingeführt. Die Bundesregierung setzt sich dafür ein, die Chatkontrolle auf europäischer Ebene zu verhindern und Ende-zu-Ende-Verschlüsselung sowie die Vertraulichkeit von Kommunikation insgesamt zu schützen.

- Eine automatisierte Datenanalyse der Informationsbestände der Strafverfolgungsbehörden sowie jede Form von Predictive Policing oder automatisiertes Profiling von Menschen wird abgelehnt. Die Kooperationen deutscher und US-Geheimdienste werden eingeschränkt, insbesondere wird jede Art von automatisiertem Massenaustausch von Inhalts- oder Metadaten unterbunden.
- Die Überwachungsgesamtrechnung wird veröffentlicht, kontinuierlich fortgesetzt und der Umfang staatlicher Überwachungsbefugnisse dementsprechend gesetzgeberisch angepasst.
- Es wird ein Recht auf Verschlüsselung eingeführt. Die Bundesregierung setzt sich dafür ein, die Chatkontrolle auf europäischer Ebene zu verhindern und Ende-zu-Ende-Verschlüsselung sowie die Vertraulichkeit von Kommunikation insgesamt zu schützen.
- IT-Sicherheitsforschung wird unterstützt statt kriminalisiert. Der Hackerparagraph wird abgeschafft. Es wird ein wirksames ITSchwachstellenmanagement auch für Behörden eingeführt. Das Bundesamt für Sicherheit in der Informationstechnik wird unabhängig aufgestellt.
- Die Bundesregierung setzt sich für wirksamen Kinder- und Jugendmedienschutz ein, ohne dabei durch eine verpflichtende Altersverifikation die Grundrechte von Kindern und Jugendlichen zu unterminieren. Die anonyme und pseudonyme Nutzung des Internets wird geschützt und ermöglicht.
- Die Abschaffung der Bezahlkarte für Geflüchtete und die Einstellung von Handyauswertungen durch das Bundesamt für Migration und Flüchtlinge. Wir fordern die Bundesregierung auf, sich auf europäischer Ebene gegen die überbordende Sammlung personenbezogener Daten geflüchteter Menschen einzusetzen und ihre Privatsphäre und Autonomie zu respektieren
- Privater Machtmissbrauch von Big-TechUnternehmen wird durch durchsetzungsstarke, unabhängige und grundsätzlich föderale Aufsichtsstrukturen bekämpft, insbesondere in den Bereichen der Plattformregulierung, des Datenschutzrechts und des Kartellrechts.
- Die Bundesregierung legt ein umfassendes Förderprogramm für digitale öffentliche Räume auf, die dezentral organisiert, gesellschaftlich eingebettet, interoperabel gestaltet und quelloffen programmiert sind.
- Ein digitales Gewaltschutzgesetz wird eingeführt, das Betroffene konsequent in den Fokus stellt. Dazu gehören auch die Reform der Impressumspflicht, die Berücksichtigung gruppenbezogener digitaler Gewalt und die Förderung von Beratungs- und Hilfsangeboten.
- Gute digitale Bildung, die Menschen befähigt und frei zugänglich ist, muss zur Priorität werden und allen gesellschaftlichen Gruppen, unabhängig von Alter und Bildungsgrad, zur Verfügung stehen.Wir fordern eine umfassende Strategie zur Förderung von Open Educational Resources und die Förderung des

- IT-Sicherheitsforschung wird unterstützt statt kriminalisiert. Der Hackerparagraph wird abgeschafft. Es wird ein wirksames IT-Schwachstellenmanagement auch für Behörden eingeführt. Das Bundesamt für Sicherheit in der Informationstechnik wird unabhängig aufgestellt.
- Die Bundesregierung setzt sich für wirksamen Kinder- und Jugendmedienschutz ein, ohne dabei durch eine verpflichtende Altersverifikation die Grundrechte von Kindern und Jugendlichen zu unterminieren. Die anonyme und pseudonyme Nutzung des Internets wird geschützt und ermöglicht.
- Die Abschaffung der Bezahlkarte für Geflüchtete und die Einstellung von Handyauswertungen durch das Bundesamt für Migration und Flüchtlinge. Wir fordern die Bundesregierung auf, sich auf europäischer Ebene gegen die Sammlung personenbezogener Daten geflüchteter Menschen einzusetzen und ihre Privatsphäre und Autonomie zu respektieren.
- Privater Machtmissbrauch von Big-Tech-Unternehmen wird durch durchsetzungsstarke, unabhängige und grundsätzlich föderale Aufsichtsstrukturen bekämpft, insbesondere in den Bereichen der Plattformregulierung, des Datenschutzrechts und des Kartellrechts.
- Die Bundesregierung legt ein umfassendes Förderprogramm für digitale öffentliche Räume auf, die dezentral organisiert, gesellschaftlich eingebettet, interoperabel gestaltet und quelloffen programmiert sind.
- Ein digitales Gewaltschutzgesetz wird eingeführt, das Betroffene konsequent in den Fokus stellt. Dazu gehören auch die Reform der Impressumspflicht, die Berücksichtigung gruppenbezogener digitaler Gewalt und die Förderung von Beratungs- und Hilfsangeboten.
- Gute digitale Bildung, die Menschen befähigt und frei zugänglich ist, muss zur Priorität werden und allen gesellschaftlichen Gruppen, unabhängig von Alter und Bildungsgrad, zur Verfügung stehen. Wir fordern eine umfassende Strategie zur Förderung von Open Educational Resources und die Förderung des digitalen Ehrenamts.
- Wir fordern eine Regelung durch die Europäische Union, die an den Marktort der Plattform anknüpft.

Begründung

Bekenntnis gegen Überwachung

Es ist ein Irrglaube, dass zunehmende Überwachung einen Zugewinn an Sicherheit darstellt. Sicherheit erfordert auch, dass Menschen anonym und vertraulich kommunizieren können und ihre Privatsphäre geschützt wird. Zu oft werden aktionistische Vorschläge wie die Chatkontrolle, Vorratsdatenspeicherung oder biometrische Überwachung als technische Allheilmittel für komplexe gesellschaftliche Herausforderungen präsentiert – ohne ihre massiven Missbrauchspotenziale zu berücksichtigen. Stattdessen braucht es eine evidenzbasierte Politik, die differenzierte Lösungsansätze ohne Massenüberwachung verfolgt. Es ist die Aufgabe des Staates, Grundrechte zu schützen. Dazu gehört insbesondere auch, den Missbrauch von Maßnahmen, Befugnissen und Infrastrukturen zu verhindern, heute und in Zukunft.

Schutz und Sicherheit für alle

IT-Angriffe wie die durch „Salt Typhoon“ zeigen die Gefahren staatlicher Hintertüren und unterstreichen: Die Stärkung von IT-Sicherheit und Ende-zu-Ende-verschlüsselter Kommunikation ist eine Frage gesamtgesellschaftlicher Resilienz. Gleichzeitig steht unabhängige und zivilgesellschaftliche Sicherheitsforschung, die Sicherheitslücken zum Wohle der Gesellschaft aufdeckt, immer noch unter Generalverdacht und wird kriminalisiert. Sicherheitslücken in Software müssen von allen staatlichen Stellen im Rahmen eines Schwachstellenmanagements konsequent an die Hersteller zur Behebung gemeldet werden. Sicherheit und Schutz dürfen dabei keine Frage von Privilegien sein, sondern müssen für alle Menschen gelten, insbesondere für marginalisierte Menschen und Gruppen.

Demokratie im digitalen Raum

Private Überwachung und Machtkonzentration müssen bekämpft werden. Die willkürliche und antidemokratische Machtausübung der Tech-Oligarchen um Präsident Trump erfordert einen Paradigmenwechsel in der deutschen Digitalpolitik und ein erneuertes Bekenntnis zu dezentralen öffentlichen Räumen sowie der konsequenten Rechtsdurchsetzung durch föderale Aufsichtsstrukturen. Gesunde digitale Räume leben auch von einer resilienten Gesellschaft mit starken digitalen Kompetenzen und einem demokratischen Diskurs, in dem digitale Gewalt keinen Platz hat. Dazu fordern wir ein Gewaltschutzgesetz, das seinen Namen verdient, einen Ausbau der digitalen Bildung und die Förderung des digitalen Ehrenamts.