

Antrag 229/I/2025

Jusos LDK

Der Landesparteitag möge beschließen:

Für eine faschismussichere Digitalpolitik

1 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:

9 Wir fordern die neue Bundesregierung auf, eine digitale Brandmauer gegen den Faschismus zu errichten. Diese digitale Brandmauer muss Missbrauchspotentiale minimieren, Menschen und gesellschaftliche Gruppen ermöglichen 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

23 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

40 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 faschismussichere 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 ermöglichen 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

49 im Rahmen eines Schwachstellenmanagements konse-
 50 quent an die Hersteller zur Behebung gemeldet werden.
 51 Sicherheit und Schutz dürfen dabei keine Frage von Pri-
 52 vilegen sein, sondern müssen für alle Menschen gelten, ins-
 53 besondere für marginalisierte Menschen und Gruppen.
 54

55 **Demokratie im digitalen Raum**

56 Private Überwachung und Machtzentration müssen
 57 bekämpft werden. Die willkürliche und antideokrati-
 58 sche Machtausübung der Tech-Oligarchen um Präsident
 59 Trump erfordert einen Paradigmenwechsel in der deut-
 60 schen Digitalpolitik und ein erneutes Bekenntnis zu de-
 61 zentralen öffentlichen Räumen sowie der konsequenten
 62 Rechtsdurchsetzung durch föderale Aufsichtsstrukturen.
 63 Gesunde digitale Räume leben auch von einer resilienten
 64 Gesellschaft mit starken digitalen Kompetenzen und ei-
 65 nem demokratischen Diskurs, in dem digitale Gewalt kei-
 66 nen Platz hat. Dazu fordern wir ein Gewaltschutzgesetz,
 67 das seinen Namen verdient, einen Ausbau der digitalen
 68 Bildung und die Förderung des digitalen Ehrenamts.
 69

70 **Wir fordern daher:**

- 71 • Die biometrische Massenüberwachung des öffentli-
 72 chen Raums sowie die ungezielte biometrische Aus-
 73 wertung des Internets wird verboten. Insbesondere
 74 wird aktiv gegen jede Form von Datenbank vorge-
 75 gangen, die ungezielt Bilder, Videos und Audiodatei-
 76 en aus dem Internet nach biometrischen Merkma-
 77 len auswertet. Die entsprechenden Befugnisse des
 78 Bundesamts für Migration und Flüchtlinge werden
 79 zurückgenommen.
- 80 • Anlasslose und massenhafte Vorratsdatenspeiche-
 81 rung wird abgelehnt. Stattdessen werden grund-
 82 rechtsschonende und effektivere Maßnahmen der
 83 Strafverfolgung wie das Quick-Freeze-Verfahren
 84 und die Login-Falle verfolgt.
- 85 • Eine automatisierte Datenanalyse der Informa-
 86 tionsbestände der Strafverfolgungsbehörden so-
 87 wie jede Form von Predictive Policing oder au-
 88 tomatisiertes Profiling von Menschen wird ab-
 89 gelehnt. Die Kooperationen deutscher und US-
 90 Geheimdienste werden eingeschränkt, insbesonde-
 91 re wird jede Art von automatisiertem Massenaus-
 92 tausch von Inhalts- oder Metadaten unterbunden.
- 93 • Die Überwachungsgesamtrechnung wird veröf-
 94 fentlicht, kontinuierlich fortgesetzt und der Umfang
 95 staatlicher Überwachungsbefugnisse dementspre-
 96 chend gesetzgeberisch angepasst.
- 97 • Es wird ein Recht auf Verschlüsselung eingeführt.
 98 Die Bundesregierung setzt sich dafür ein, die Chat-
 99 kontrolle auf europäischer Ebene zu verhindern und
 100 Ende-zu-Ende-Verschlüsselung sowie die Vertrau-
 101 lichkeit von Kommunikation insgesamt zu schützen.

Inhalts- oder Metadaten unterbunden.

- Die Überwachungsgesamtrechnung wird veröf-
 fentlicht, kontinuierlich fortgesetzt und der Umfang
 staatlicher Überwachungsbefugnisse dementspre-
 chend gesetzgeberisch angepasst.
- Es wird ein Recht auf Verschlüsselung eingeführt.
 Die Bundesregierung setzt sich dafür ein, die Chat-
 kontrolle auf europäischer Ebene zu verhindern und
 Ende-zu-Ende-Verschlüsselung sowie die Vertrau-
 lichkeit von Kommunikation insgesamt zu schützen.
- IT-Sicherheitsforschung wird unterstützt statt kri-
 minalisiert. Der Hackerparagraph wird abgeschafft.
 Es wird ein wirksames IT-Schwachstellenmanage-
 ment auch für Behörden eingeführt. Das Bundes-
 amt für Sicherheit in der Informationstechnik wird
 unabhängig aufgestellt.
- Die Bundesregierung setzt sich für wirksamen
 Kinder- und Jugendmedienschutz ein, ohne da-
 bei durch eine verpflichtende Altersverifikation die
 Grundrechte von Kindern und Jugendlichen zu un-
 terminieren. Die anonyme und pseudonyme Nut-
 zung 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 europäi-
 scher Ebene gegen die überbordende Sammlung
 personenbezogener Daten geflüchteter Menschen
 einzusetzen und ihre Privatsphäre und Autonomie
 zu respektieren
- Privater Machtmissbrauch von Big-
 Tech-Unternehmen wird durch durchsetzungs-
 starke, unabhängige und grundsätzlich föderale
 Aufsichtsstrukturen bekämpft, insbesondere in
 den Bereichen der Plattformregulierung, des
 Datenschutzrechts und des Kartellrechts.
- Die Bundesregierung legt ein umfassendes Förder-
 programm für digitale öffentliche Räume auf, die
 dezentral organisiert, gesellschaftlich eingebettet,
 interoperabel gestaltet und quelloffen progra-
 miert sind.
- Ein digitales Gewaltschutzgesetz wird eingeführt,
 das Betroffene konsequent in den Fokus stellt. Dazu
 gehören auch die Reform der Impressumspflicht, die
 Berücksichtigung gruppenbezogener digitaler Ge-
 walt und die Förderung von Beratungs- und Hilfsan-
 geboten.
- Gute digitale Bildung, die Menschen befähigt und
 frei zugänglich ist, muss zur Priorität werden und al-
 len gesellschaftlichen Gruppen, unabhängig von Alter
 und Bildungsgrad, zur Verfügung stehen. Wir for-
 dern eine umfassende Strategie zur Förderung von
 Open Educational Resources und die Förderung des

- 102 • IT-Sicherheitsforschung wird unterstützt
103 statt kriminalisiert. Der Hackerparagraph
104 wird abgeschafft. Es wird ein wirksames IT-
105 Schwachstellenmanagement auch für Behörden
106 eingeführt. Das Bundesamt für Sicherheit in der
107 Informationstechnik wird unabhängig aufgestellt.
- 108 • Die Bundesregierung setzt sich für wirksamen
109 Kinder- und Jugendmedienschutz ein, ohne da-
110 bei durch eine verpflichtende Altersverifikation die
111 Grundrechte von Kindern und Jugendlichen zu un-
112 terminieren. Die anonyme und pseudonyme Nut-
113 zung des Internets wird geschützt und ermöglicht.
- 114 • Die Abschaffung der Bezahlkarte für Geflüchtete
115 und die Einstellung von Handyauswertungen durch
116 das Bundesamt für Migration und Flüchtlinge. Wir
117 fordern die Bundesregierung auf, sich auf europäi-
118 scher Ebene gegen die Sammlung personenbezoge-
119 ner Daten geflüchteter Menschen einzusetzen und
120 ihre Privatsphäre und Autonomie zu respektieren.
- 121 • Privater Machtmissbrauch von Big-Tech-
122 Unternehmen wird durch durchsetzungsstarke,
123 unabhängige und grundsätzlich föderale Auf-
124 sichtsstrukturen bekämpft, insbesondere in den
125 Bereichen der Plattformregulierung, des Daten-
126 schutzrechts und des Kartellrechts.
- 127 • Die Bundesregierung legt ein umfassendes Förder-
128 programm für digitale öffentliche Räume auf, die
129 dezentral organisiert, gesellschaftlich eingebettet,
130 interoperabel gestaltet und quelloffen program-
131 miert sind.
- 132 • Ein digitales Gewaltschutzgesetz wird eingeführt,
133 das Betroffene konsequent in den Fokus stellt. Dazu
134 gehören auch die Reform der Impressumspflicht, die
135 Berücksichtigung gruppenbezogener digitaler Ge-
136 walt und die Förderung von Beratungs- und Hilfsan-
137 geboten.
- 138 • Gute digitale Bildung, die Menschen befähigt und
139 frei zugänglich ist, muss zur Priorität werden und al-
140 len gesellschaftlichen Gruppen, unabhängig von Al-
141 ter und Bildungsgrad, zur Verfügung stehen. Wir for-
142 dern eine umfassende Strategie zur Förderung von
143 Open Educational Resources und die Förderung des
144 digitalen Ehrenamts.
- 145 • Wir fordern eine Regelung durch die Europäische
146 Union, die an den Marktort der Plattform anknüpft.

147 digitalen Ehrenamts.

Begründung

Bekenntnis gegen Überwachung

163 Es ist ein Irrglaube, dass zunehmende Überwachung
164 einen Zugewinn an Sicherheit darstellt. Sicherheit er-
165 fordert auch, dass Menschen anonym und vertraulich
166 kommunizieren können und ihre Privatsphäre geschützt
167 wird. Zu oft werden aktionistische Vorschläge wie die
168 Chatkontrolle, Vorratsdatenspeicherung oder biometri-
169 sche Überwachung als technische Allheilmittel für kom-
170 plexe gesellschaftliche Herausforderungen präsentiert –
171 ohne ihre massiven Missbrauchspotenziale zu berücksich-
172 tigen. Stattdessen braucht es eine evidenzbasierte Politik,
173 die differenzierte Lösungsansätze ohne Massenüberwa-
174 chung verfolgt. Es ist die Aufgabe des Staates, Grundrech-
175 te zu schützen. Dazu gehört insbesondere auch, den Miss-
176 brauch von Maßnahmen, Befugnissen und Infrastruktu-
177 ren zu verhindern, heute und in Zukunft.

Schutz und Sicherheit für alle

178 IT-Angriffe wie die durch „Salt Typhoon“ zeigen die Gefah-
179 ren staatlicher Hintertüren und unterstreichen: Die Stär-
180 kung von IT-Sicherheit und Ende-zu-Ende-verschlüsselter
181 Kommunikation ist eine Frage gesamtgesellschaftlicher
182 Resilienz. Gleichzeitig steht unabhängige und zivilgesell-
183 schaftliche Sicherheitsforschung, die Sicherheitslücken
184 zum Wohle der Gesellschaft aufdeckt, immer noch un-
185 ter Generalverdacht und wird kriminalisiert. Sicherheits-
186 lücken in Software müssen von allen staatlichen Stellen
187 im Rahmen eines Schwachstellenmanagements konse-
188 quent an die Hersteller zur Behebung gemeldet werden.
189 Sicherheit und Schutz dürfen dabei keine Frage von Pri-
190 ligien sein, sondern müssen für alle Menschen gelten, ins-
191 besondere für marginalisierte Menschen und Gruppen.

Demokratie im digitalen Raum

192 Private Überwachung und Machtkonzentration müssen
193 bekämpft werden. Die willkürliche und antidemokrati-
194 sche Machtausübung der Tech-Oligarchen um Präsident
195 Trump erfordert einen Paradigmenwechsel in der deut-
196 schen Digitalpolitik und ein erneuertes Bekenntnis zu de-
197 zentralen öffentlichen Räumen sowie der konsequenten
198 Rechtsdurchsetzung durch föderale Aufsichtsstrukturen.
199 Gesunde digitale Räume leben auch von einer resilienten
200 Gesellschaft mit starken digitalen Kompetenzen und ei-
201 nem demokratischen Diskurs, in dem digitale Gewalt kei-
202 nen Platz hat. Dazu fordern wir ein Gewaltschutzgesetz,
203 das seinen Namen verdient, einen Ausbau der digitalen
204 Bildung und die Förderung des digitalen Ehrenamts.