

Antrag 103/II/2023

Forum Netzpolitik

Der Landesparteitag möge beschließen:

Der Bundesparteitag möge beschließen:

Empfehlung der Antragskommission

Überweisen an: ASJ, FA III - Innen- und Rechtspolitik (Konsens)

Ein starkes Recht auf Verschlüsselung zum Schutz der Bürger:innen und sensibler Unternehmensdaten

1 Die Mitglieder der SPD-Fraktion im Bundestag und des
2 Europaparlaments werden aufgefordert, folgenden Be-
3 schluss umzusetzen:

4
5 Wir bekennen uns klar zum Recht auf sichere Kommunika-
6 tion und wirksame Verschlüsselung für alle Bürger:innen,
7 Unternehmen und Institutionen: Als Bürger:innen haben
8 wir das Recht, unsere persönlichen Informationen, Kom-
9 munikation und Daten durch Nutzung von Verschlüsse-
10 lungstechnologien vor unbefugtem Zugriff zu schützen.
11 Wir verlangen, dass das im Koalitionsvertrag auf Bundes-
12 ebene vereinbarte Recht auf Verschlüsselung ohne Ein-
13 schränkungen auf Bundes- und EU-Ebene umgesetzt wird.

14
15 Starke Verschlüsselungstechnologien werden aufgrund
16 der zunehmenden Digitalisierung aller Lebensbereiche
17 immer wichtiger. Sie schützen unsere private Kommu-
18 nikation und persönliche Daten, schützen vor Massen-
19 überwachung und Cyberkriminalität. Wir verlangen da-
20 her, dass die Politik Maßnahmen ergreift, um sicherzu-
21 stellen, dass die Lebensbereiche online genauso geschützt
22 sind wie offline.

23
24 Zum Recht auf sichere Kommunikation und wirksame Ver-
25 schlüsselung gehört auch der Schutz der Kommunikation
26 vor staatlicher Kontrolle. Eine Aufweichung oder Aushe-
27 belung der Ende-zu-Ende-Verschlüsselung durch freiwilli-
28 ges oder verpflichtendes Client-Side-Scanning bei Anbie-
29 tern verschlüsselter Kommunikationsplattformen ist da-
30 her nicht akzeptabel.

31
32 Im Einzelnen werden wir uns für die folgenden Punkte ein-
33 setzen:

34 1. Das grundlegende Schutzniveau muss gestärkt statt
35 abgeschwächt werden: Es ist der staatliche Auf-
36 trag, die Schutzmechanismen aller zu erhöhen, statt
37 sie zu begrenzen oder abzuschwächen. Regulierun-
38 gen, die den Einbau von staatlichen Hintertüren
39 als „goldene Schlüssel“ in Verschlüsselungstechnik
40 oder andere generelle Abschwächungen des Schutz-
41 niveaus mit sich bringen würden, etwa zur Bekämp-
42 fung von Kriminalität, lehnen wir ab. Aktivitäten
43 auf Bundes- oder EU-Ebene, die Verschlüsselung
44 schwächen und umgehen, sind unzulässig, da sie
45 die Sicherheit aller Bürger:innen und unserer Wirt-
46 schaft einem enormen Risiko aussetzen. Entspre-
47 chend werden auch aktuelle Bestrebungen auf EU-

- 48 Ebene abgelehnt, die im Rahmen einer hochrangi-
49 gigen Expertengruppe (HLEG) im Juni 2023 durch die
50 Ratspräsidentschaft eingerichtet wurde und techni-
51 sche Vorschläge für eine Regulierung zu Kryptoprod-
52 ukten und -diensten zu entwickeln.
- 53 2. Wir wollen die technische Verfügbarkeit von Vers-
54 schlüsselungstechnologie sicherstellen und erhö-
55 hen: Auf EU- und Bundesebene sollen künftig ge-
56 zielt Open-Source-Projekte gefördert werden, die
57 sich auf sichere Kommunikation und Verschlüsse-
58 lungstechnologien konzentrieren oder sie beinhal-
59 ten. Das erfolgt insbesondere durch finanzielle
60 Mittel, Wettbewerbe, Auszeichnungen und Beloh-
61 nungssysteme für die Suche nach Softwarefeh-
62 lern (Bug Bounty). In dem Zusammenhang sollen
63 auch Partnerschaften mit Unternehmen und Or-
64 ganisationen der Zivilgesellschaft gefördert wer-
65 den. Forschungsprojekte im Bereich der Verschlüs-
66 selung sollen stärker gefördert werden. Wir un-
67 terstützen die Entwicklung und Nutzung von si-
68 cheren Kommunikations-Plattformen, die Ende-zu-
69 Ende-Verschlüsselung bieten. Im Rahmen einer of-
70 fenen Beschaffungspolitik müssen Lösungen für si-
71 chere und verschlüsselte Kommunikation, die auf
72 offenen Standards und Open Source basieren, bei
73 der Beschaffung von Software und Technologie für
74 staatliche Einrichtungen bevorzugt werden. Zusätz-
75 lich müssen Maßnahmen ergriffen werden, damit
76 entsprechende Software-Projekte durch Förderung,
77 Sandbox-Nutzungen in Behörden etc. entsprechen-
78 de Marktreife erreichen können.
- 79 3. Kampagnen zur Sensibilisierung und Aufklärung
80 über die Vorteile von sicherer Kommunikation und
81 Verschlüsselung und die Bedeutung der digitalen
82 Sicherheit für Bürger:innen, mittelständische Un-
83 ternehmen, Freiberufler:innen und Organisationen
84 der Zivilgesellschaft, mit dem Ziel der stärkeren
85 Nutzung entsprechender Technologien. Verschlüs-
86 selung muss die Regel werden, darf nicht die Aus-
87 nahme bleiben.
- 88 4. Starke Verschlüsselung als außenpolitisches Mittel
89 zum weltweiten Schutz vor Zensur und Unterdrü-
90 ckung: Starke Verschlüsselung ermöglicht es Men-
91 schen, vertraulich und sicher miteinander zu kom-
92 munizieren, ohne Angst vor Überwachung oder Re-
93 pressalien zu haben. Dies ist besonders wichtig in
94 Ländern mit restriktiven Regimen, in denen die Mei-
95 nungsfreiheit eingeschränkt ist. Menschen in zen-
96 sierten Ländern helfen diese Techniken, auf Infor-
97 mationen und Nachrichten zuzugreifen, die sonst
98 durch Zensurbehörden blockiert würden. Entspre-
99 chend sind diplomatische Kanäle zu nutzen, inter-
100 nationale Foren genutzt werden, Aktivist:innen und

101 Zivilgesellschaft in entsprechenden Ländern Unter-
102 stützung angeboten werden.
103 5. Kommunikation und persönliche Daten müssen be-
104 reits heute durch zukunftstaugliche quantenresis-
105 tente kryptografische Verfahren abgesichert wer-
106 den: Angriffe auf heutige Verschlüsselungstechnik
107 werden im Laufe der Zeit immer besser. Damit heu-
108 te verschlüsselte Daten auch bei der Verfügbarkeit
109 von Quantencomputern geschützt bleiben, muss
110 Kommunikation bereits heute durch quantenresis-
111 tente kryptografische Verfahren abgesichert wer-
112 den. Insbesondere Bürger:innen, mittelständische
113 Unternehmen, Freiberufler:innen und Organisatio-
114 nen der Zivilgesellschaft sind über quantenresis-
115 tente Kommunikation und Speicherung aufzuklä-
116 ren und deren Einsatz ist zu fördern.

117

118

119 **Begründung**

120 Die Vertraulichkeit und Sicherheit der digitalen Kommu-
121 nikation sind für unsere Gesellschaft unverzichtbar. Nicht
122 nur der demokratische Diskurs lebt vom freien Meinungs-
123 austausch, sondern auch unsere Wirtschaft benötigt si-
124 chere Kommunikation. Schließlich erfordert auch die Digi-
125 talisierung unserer staatlichen Verwaltung ein hohes Maß
126 an Vertrauen in IT-Infrastrukturen.

127 Wir befinden uns zudem in einem „goldenen Zeitalter“
128 der enormen Verfügbarkeit von Daten für öffentliche und
129 private Akteure. Daten müssen daher stärker geschützt
130 werden, auch vor von Ermittlungsbehörden gerne gefor-
131 derten staatlichen Zugriffen.

132 Zu Ziff. 1 (Schutzniveau stärken):

133 Die Sicherstellung und Erhöhung der Verfügbarkeit si-
134 cherer Verschlüsselungstechnologie ist entscheidend, um
135 die Privatsphäre und den Schutz sensibler Informationen
136 für Bürger und Unternehmen zu gewährleisten. Sie trägt
137 zur Abwehr von Cyberangriffen, Identitätsdiebstahl und
138 Überwachung bei, während sie gleichzeitig die Meinungs-
139 freiheit und den freien Informationsfluss in einer vernetz-
140 ten Welt unterstützt. Die Aufgabe, Kriminalität und Ter-
141 rorismus zu bekämpfen, darf nicht dazu genutzt werden,
142 die grundlegenden Schutzmechanismen zu untergraben.
143 Behörden müssen stärker auf moderne Ermittlungsm-
144 ethoden setzen und darin unterstützt werden, als die IT-
145 Sicherheit aller durch Regulierung herabzusetzen.

146 Zu Ziff. 2 (Verfügbarkeit von Verschlüsselungstechno-
147 logie):

148 Die Sicherstellung und Steigerung der technischen Ver-
149 fügbarkeit von Verschlüsselungstechnologie ist essenzi-
150 ell, um die digitale Sicherheit und Privatsphäre der Bürger
151 zu schützen. Open Source ist dabei als Ansatz besonders
152 wichtig, da es Transparenz und Überprüfbarkeit fördert,
153 was das Vertrauen in die Sicherheit der Produkte erhöht

154 und Hintertüren oder Schwachstellen minimiert, die von
155 Dritten missbraucht werden könnten.

156 Zu Ziff. 3 (Kampagnen zur Sensibilisierung und Aufklä-
157 rung):

158 Informationskampagnen zur Sensibilisierung und Aufklä-
159 rung sind unerlässlich, um Bürger:innen und Unterneh-
160 men für die richtige Anwendung von Verschlüsselung zu
161 sensibilisieren, sie vor Fehlanwendungen zu schützen und
162 so die digitale Sicherheitskultur zu stärken.

163 Zu Ziff. 4 (Starke Verschlüsselung als außenpolitisches
164 Mittel):

165 Bedrohte Aktivist:innen in undemokratischen Ländern
166 sind auf verschlüsselte Kommunikation und sicheres Sur-
167 fen angewiesen, um sich vor Überwachung und Verfol-
168 gung zu schützen. Aktuelle Beispiele wie die Verwendung
169 von Messaging-Apps mit Ende-zu-Ende-Verschlüsselung
170 während der Proteste in Hongkong oder die Nutzung von
171 VPNs (Virtual Private Networks) durch Aktivist:innen im
172 Iran zeigen, wie diese Technologien helfen können, ihre
173 Identität zu wahren, Informationen sicher auszutauschen
174 und die globale Öffentlichkeit über Menschenrechtsver-
175 letzungen aufzuklären.

176 Zu Ziff. 5 (Quantenresistente kryptografische Verfahren):

177 Angriffe auf etablierte Verschlüsselungsalgorithmen wer-
178 den im Laufe der Zeit immer besser, sodass es regelmä-
179 ßig erforderlich ist, auf stärkere Verfahren umzusteigen.
180 Vor allem die Entwicklung von Quantencomputern stellt
181 eine Gefahr dar, da diese in der Lage sind, Berechnungen
182 hocheffizient auszuführen, die für die derzeitigen Rechen-
183 methoden unerreichbar sind. Diesbezüglich wurden mo-
184 derne Verschlüsselungsansätze wie der hybride Schlüssel-
185 kapselungsmechanismus (KEM) vom US-Institut NIST zu
186 einem sicheren Kandidaten im Hinblick auf quantenresis-
187 tente Kryptografie erklärt.

188 Auch wenn entsprechend leistungsfähige Quantencom-
189 puter wohl erst in mehreren Jahren oder Jahrzehnten zur
190 Verfügung stehen werden, ist es wichtig, schon jetzt Maß-
191 nahmen zu ergreifen. Denn das Fehlen von quantenre-
192 sistenten kryptografischen Verfahren motiviert Angreifer,
193 potenziell wertvolle Daten schon heute in verschlüsselter
194 Form zu sammeln und sie erst zu knacken, sobald entspre-
195 chende Rechner verfügbar sind.