

**Antrag 215/II/2019****ASJ Landesvorstand + Forum Netzpolitik****Der Landesparteitag möge beschließen:****Der Bundesparteitag möge beschließen:****Empfehlung der Antragskommission****Annahme (Konsens)****IT-Sicherheit stärken und digitale Freiheit schützen (IT-Sicherheitsgesetz 2.0)**

1 Unser Grundgesetz garantiert eine Reihe von Bür-  
2 ger\*innen- und Freiheitsrechte, welche dem Eingriff des  
3 Staates in die freie und umfassende Entfaltung der eige-  
4 nen Persönlichkeit Grenzen setzen. Dazu gehören neben  
5 dem Fernmeldegeheimnis auch die Unverletzlichkeit der  
6 Wohnung und das Grundrecht auf Gewährleistung der  
7 Vertraulichkeit und Integrität informationstechnischer  
8 Systeme (IT-Grundrecht). Leider wird die zunehmende  
9 Digitalisierung aller Lebensbereiche immer öfter zum  
10 Vorwand genommen, die Grundrechte mehr und mehr  
11 einzuschränken, oft mit dem Argument eines vermeint-  
12 lichen Sicherheitsgewinns. Die Digitalisierung darf nicht  
13 zum Reflex führen, im digitalen Raum Freiheitsrechte  
14 stärker einzuschränken, als in der analogen Welt. Viel-  
15 mehr müssen wir auch in der digitalen Welt unsere  
16 Freiheiten schützen.

17  
18 Eingriffe in das informationelle Selbstbestimmungsrecht  
19 und in die Vertraulichkeit digitaler Systeme dürfen auch  
20 im digitalen Netz nur nach strengen gesetzlichen Vor-  
21 gaben erfolgen. Das digitale Netz ist aber kein rechts-  
22 freier Raum, auch im Netz müssen Straftaten aufgeklärt  
23 und verfolgt, Gefahren erkannt und beseitigt werden.  
24 Strafverfolgungsmaßnahmen dürfen aber nur bei einem  
25 konkreten Anfangsverdacht, Gefahrenabwehrmaßnah-  
26 men nur bei einem konkreten Gefahrenverdacht und bei-  
27 des mit Richtervorbehalt zugelassen werden. Der nemo-  
28 tenetur-Grundsatz, die Grundrechte und der Grundsatz  
29 der Verhältnismäßigkeit müssen uneingeschränkt gelten  
30

31 Mit Blick auf das kommende IT-Sicherheitsgesetz 2.0 for-  
32 dern wir daher:

33

**34 1. Recht auf Verschlüsselung und Anonymität**

35 Niemand darf unter einen Generalverdacht gestellt wer-  
36 den, weil er vertrauliche und sichere Kommunikations-  
37 wege nutzt oder sie anderen zur Nutzung bereitstellt. In  
38 Zeiten der weltweit steigenden staatlichen Einflussnah-  
39 me auf die Funktionsweise und Inhalte zentraler Netz-  
40 werkdienste, darf die Nutzung verschlüsselter, dezentra-  
41 ler und/oder anonymer Kommunikationswege nicht kri-  
42 minalisiert werden, sondern sollte gefördert werden. Für  
43 viele Menschen weltweit sind starke Verschlüsselungs-  
44 methoden, das TOR-Netzwerk („Darknet“) sowie andere  
45 dezentrale Kommunikationswege essenziell, um die Ge-  
46 fahr von Stigmatisierung oder staatlicher Repression zu  
47 umgehen.

48 Gesetzesverschärfungen, die das Zugänglichmachen ent-  
49 sprechender internetbasierter Leistungen oder das Er-  
50 leichtern von Straftaten unter Strafe stellen, lehnen wir  
51 ab. Diese Dienste dienen insbesondere auch Journalist\*in-  
52 nen und Whistleblowern, die unter teils hohen persönli-  
53 chen Risiken für die Allgemeinheit wichtige Informatio-  
54 nen aus einem geheimen oder geschützten Zusammen-  
55 hang an die Öffentlichkeit bringen. Aber auch unabhän-  
56 gig von besonderen beruflichen Geheimhaltungspflich-  
57 ten und -interessen gilt, dass alle Bürger\*innen ein Recht  
58 auf verschlüsselte Kommunikation haben und dieses we-  
59 der im Einzelfall noch generell rechtfertigen oder begrün-  
60 den müssen. Messenger-Dienste wie Whatsapp/Telegram  
61 sollten ihre Daten zum Schutz der Nutzer\*innen ohne Hin-  
62 tertüren verschlüsseln dürfen.

63

## 64 **2. Kein Zwang zur Herausgabe von Passwörtern**

65 Das Verbot des Zwangs zur Selbstbelastung und die Aus-  
66 sagefreiheit des Beschuldigten sind im Grundgesetz ver-  
67 ankert. Sie sind Ausdruck einer auf der Achtung der  
68 Menschenwürde beruhenden rechtsstaatlichen Grund-  
69 haltung. Niemand muss sich selbst belasten. Dieser  
70 Grundsatz muss auch im digitalen Raum gelten. Einen  
71 Zwang zur Herausgabe von Passwörtern oder anderen Zu-  
72 gangsdaten unter Androhung von Beugehaft, lehnen wir  
73 als verfassungswidrig ab. Auch die Übernahme von Nut-  
74 zerkonten durch staatliche Behörden gegen den Willen  
75 des Inhabers und die Kontaktaufnahme ggü. Dritten über  
76 dieses Konto lehnen wir als unverhältnismäßig ab. Eben-  
77 so lehnen wir die Pläne ab, den Strafverfolgungsbehörden  
78 anderer EU-Mitgliedstaaten im Rahmen der derzeit auf  
79 EU-Ebene verhandelten E-Evidence-Verordnung zu erlau-  
80 ben, Zugangsdaten bei Providern in Deutschland und in  
81 anderen Mitgliedstaaten sowie Drittstaaten mittels einer  
82 Herausgabeanordnung zu erlangen.

83

## 84 **3. Forschung zur IT-Sicherheit und -Schwachstellen nicht** 85 **kriminalisieren, sondern fördern**

86 Die Arbeit der IT-Sicherheits- und Schwachstellenfor-  
87 schung ist ein essenzieller Beitrag für eine starke IT-  
88 Sicherheit und sollte durch Anreizsysteme, wie Bug-  
89 Bounty-Programme, gefördert werden. Aktuelle Forde-  
90 rungen nach Einführung eines Tatbestands des "digita-  
91 len Hausfriedensbruchs", der bereits die unbefugte In-  
92 gebrauchnahme informationstechnischer Systeme unter  
93 Freiheitsstrafe stellen möchte lehnen wir ab, da auch  
94 eine Vielzahl alltäglicher Vorgänge betroffen wäre. Es  
95 gilt, Rechtsunsicherheiten zu reduzieren, statt neue zu  
96 erschaffen. Auch Reverse Engineering, also die Analyse  
97 geschlossener Hard- oder Software, indem „rückwärts“  
98 der enthaltene Quellcode extrahiert wird, sollte gefördert  
99 werden.

100

101 **4. Weiterentwicklung des Bundesamts für Sicherheit in**  
102 **der Informationstechnik (BSI) zu einer unabhängigen, de-**  
103 **fensiven und neutralen Stelle für IT-Sicherheit**

104

105 **4a) Weiterentwicklung des BSI - endlich Unabhängigkeit**

106 Aufgrund der vorgegebenen Interessenkonflikte zwischen  
107 Belangen der inneren Sicherheit und denen der Sicherheit  
108 und Integrität informationsverarbeitender Systeme, muss  
109 das BSI in Anbetracht seiner wachsenden Relevanz aus der  
110 fachlichen Weisungsgebundenheit des Bundesministers  
111 des Innern, für Heimat und Bau herausgelöst werden. Das  
112 könnte z. B. durch Anknüpfung an die Stelle des Bundesda-  
113 tenschutzbeauftragten oder durch eine vergleichbare or-  
114 ganisatorische Ausgestaltung erreicht werden.

115

116 **4b) Das BSI sollte eine neutrale und defensive Stelle für**  
117 **IT-Sicherheit bleiben und darf nicht selbst zum Angreifer**  
118 **werden**

119 Die Rolle des BSI als neutrale und defensive Stelle für IT-  
120 Sicherheit zu Gunsten von Bürger\*innen und Unterneh-  
121 men darf nicht vermischt werden mit staatlichen Verfol-  
122 gungsinteressen. Dazu muss, z.B. im IT-Sicherheitsgesetz  
123 2.0, eine Bindung der gewonnenen Erkenntnisse und Da-  
124 ten an defensive Zwecke vorgeschrieben werden. Eine  
125 Mischlösung, nach denen das BSI Informationen, die es im  
126 Vertrauen auf seine Neutralität erhalten hat, für sich oder  
127 andere Behörden zurückhält um damit staatliche Eingriffe  
128 zu ermöglichen, lehnen wir ab.

129

130 **Begründung**

131 Der Antrag ist aus Anlass des BMI-Entwurfs für das sog. IT-  
132 Sicherheitsgesetz 2.0 (s. Link unten) entstanden, gilt aber  
133 grundsätzlich und über diesen Anlass hinaus für ein aus-  
134 gewogenes Verhältnis zwischen Sicherheit und Freiheit  
135 im digitalen Raum.

136

137 **Zu 1. Recht auf Verschlüsselung und Anonymität**

138 Es gibt viele gute Gründe, warum Nutzer\*innen ihre Da-  
139 ten oder Kommunikation verschlüsseln und/oder anony-  
140 misieren wollen/müssen. Der Staat sollte die Bürger\*in-  
141 nen dabei unterstützen und sie nicht kriminalisieren. Wer  
142 die Entschlüsselung von Nachrichten durch Messenger-  
143 Anbietern verlangt, würde sie dazu zwingen, absicht-  
144 lich Schwachstellen in der Technik einbauen zu müs-  
145 sen. Der Hinweis auf Straftaten, die unter Zurhilfenah-  
146 me von Verschlüsselungstechniken wie dem sog. "Dark  
147 Net" erfolgen, kann dem Staat nicht als Argument die-  
148 nen, diese Selbstschutz-Maßnahmen unter einen Gene-  
149 ralverdacht oder gar unter Strafe zu stellen. Die aktuellen  
150 diesbzgl. Bestrebungen wie im Entwurf des BMI für das  
151 IT-Sicherheitsgesetz 2.0 in einem § 126a StGB-E, bereits  
152 auch das Zugänglichmachen entsprechender internetba-  
153 sierter Leistungen unter Strafe stellen, sind daher der fal-

154 sche Weg. Auch im Bereich des sogenannten „Darknet“  
155 konnten Ermittlungsbehörden in der Vergangenheit gro-  
156 ße Fahndungserfolge erzielen, sodass eine generelle Kri-  
157 minalisierung des Einsatzes solcher Dienste nicht erfor-  
158 derlich ist. Plattformbetreiber, auf dessen Plattform die  
159 Waffe des Münchner Attentäters gekauft wurde, ist u.a.  
160 wegen Beihilfe zu unerlaubtem Handeltreiben mit einer  
161 Schusswaffe und zum vorsätzlichen unerlaubten Handel-  
162 treiben mit einer Schusswaffe in Tateinheit mit fahrlässi-  
163 ger Tötung in neun Fällen in weiterer Tateinheit mit fahr-  
164 lässiger Körperverletzung in fünf Fällen, verurteilt wor-  
165 den.

166 Mit großer Sorge ist zudem international zu beobachten,  
167 wie mehr und mehr Staaten Angst vor den Frei-  
168 heiten des Internets ihre Netze regionalisieren. China ist  
169 dort mit seiner „großen Firewall“ bereits fast am Ziel einer  
170 totalen Überwachung der Inhalte angekommen. Russland  
171 wird nun mit seinem „Gesetz über das souveräne Inter-  
172 net“ versuchen, einen ähnlichen Weg einzuschlagen. Wei-  
173 tere Länder eifern ebenfalls nach und können dafür z.B.  
174 hoch effiziente Überwachungstechnik aus China erwer-  
175 ben.

176

177 **Zu 2.** Im Entwurf des BMI zum IT-Sicherheitsgesetz 2.0  
178 wird in § 163g StPO-E vorgeschlagen, verdächtige Men-  
179 schen gesetzlich zu verpflichten, Zugangsdaten zur Nut-  
180 zung virtueller Identitäten herauszugeben. Diese Ver-  
181 pflichtung soll gegen den Willen des Verpflichteten auch  
182 mit Zwangsmitteln durchsetzbar sein, d.h. per Ordnungs-  
183 geld oder Haft von bis zu 6 Monaten. In der Praxis könnte  
184 es somit dazu kommen, dass ein Verdächtiger ins Gefäng-  
185 nis muss, weil er seine Passwörter nicht herausgibt.

186 Juristen halten diesen Ansatz für höchst problematisch  
187 und für einen Verstoß gegen den Grundsatz der Freiheit,  
188 sich nicht selbst belasten zu müssen. Strafverteidiger Udo  
189 Vetter hält das in einem SZ-Interview (9.4.2019) für ei-  
190 nen „krassen Systembruch und eine der weitest gehen-  
191 den Aufweichungsversuche der Bürgerrechte überhaupt.“  
192 Auch Zeugen könnten bislang die Herausgabe verweigern,  
193 wenn sie befürchteten, sich dadurch verdächtig zu ma-  
194 chen.

195

196 **Zu 3.** Der im BMI-Entwurf zum IT-Sicherheitsgesetz 2.0  
197 als § 200e StGB-E vorgesehene Straftatbestand, der  
198 u.a. die unbefugte Ingebrauchnahme informationstechni-  
199 scher Systeme unter Freiheitsstrafe stellen möchte, ist ab-  
200 zulehnen. Der Tatbestand ist so ungenau definiert, dass  
201 viele Analysetätigkeiten ohne Schädigungsabsicht künf-  
202 tig in einem rechtlichen Graubereich erfolgen müssten.  
203 Sog. Hacker-Tools sind notwendig, um die Sicherheit von  
204 Systemen zu testen und zu erhöhen. Dafür ist auch das  
205 sog. Reverse Engineering wichtig, das ein wichtiges Instru-  
206 ment der Sicherheitsforschung, aber auch bei der Weiter-

207 entwicklung neuer Software ist.  
208 **Zu 4. 4b** des BMI-Entwurfs zum IT-Sicherheitsgesetz 2.0  
209 beschreibt die Aufgaben des Bundesamts für Sicherheit in  
210 der Informationstechnik (BSI). Eine Bindung der gewonne-  
211 nen Erkenntnisse und Daten an defensive Zwecke ist dort  
212 nicht enthalten. Gleichzeitig erhält der Staat immer mehr  
213 nicht-defensive Befugnisse, wie die Nutzung von Staats-  
214 trojanern oder die Diskussionen zu sog. Hackbacks zeigen.  
215 Schwachstellenforscher\*innen können sich somit nicht  
216 mehr sicher sein, ob BSI umgehend veranlasst, dass ge-  
217 meldete Schwachstellen an die Hersteller gemeldet wer-  
218 den, oder ob Schwachstellen wie von den amerikanischen  
219 Geheimdiensten bekannt, teilweise auch bewusst nicht  
220 beseitigt werden, um diese für nicht-defensive Maßnah-  
221 men für einen gewissen Zeitraum auszunutzen. Dieses  
222 Vertrauen sollte aber bestehen.  
223  
224 **Link zum Gesetzesentwurf: <https://netzpo->**  
225 **litik.org/2019/it-sicherheitsgesetz-2-0-wir-**  
226 **veroeffentlichen-den-entwurf-der-das-bsi-zur-**  
227 **hackerbehoerde-machen-soll**