

Antrag 306/I/2020**Forum Netzpolitik****Der Landesparteitag möge beschließen:****Der Bundesparteitag möge beschließen:****Empfehlung der Antragskommission****Annahme****Grundrechte achten: Quellen-TKÜ begrenzen, Überwachungsgesetze evaluieren**

- 1 Die sozialdemokratischen Mitglieder der Bundesregie-
2 rung werden aufgefordert:
- 3 1. Die Nutzung sogenannter Staatstrojaner,
4 staatlich entwickelter oder anderweitig be-
5 schaffter Schadsoftware für die Quellen-
6 Telekommunikationsüberwachung (Q-
7 TKÜ) digitaler Endgeräte, muss auf die Polizei-
8 behörden beschränkt bleiben. Eine zusätzliche
9 Ausweitung der Befugnisse auf das Bundesamt für
10 Verfassungsschutz, den Militärischen Abschirm-
11 dienst, den Bundesnachrichtendienst, sowie die
12 16 bundesdeutschen Landesämter für Verfassungs-
13 schutz lehnen wir ab. Dies gilt erst Recht für die
14 noch weitergehende Onlinedurchsuchung. Die
15 Nutzung der Quellen-TKÜ durch Polizeibehörden
16 sollte kritisch hinterfragt werden.
- 17 2. Mitwirkungspflichten für Provider müssen auf ein
18 Maß begrenzt bleiben, das die neutrale Mittlerrol-
19 le und das Vertrauensverhältnis zwischen Providern
20 und Kund*innen wahrt und Verschlüsselung unan-
21 getastet lässt. Insbesondere das Umleiten von Da-
22 tenflüssen zum unbemerkten Einspielen von Schad-
23 software zur Überwachung ist grundsätzlich abzu-
24 lehnen.
- 25 3. Der Einsatz von Q-TKÜ ist aus verfassungsrechtli-
26 chen Gründen, unabhängig von der durchführenden
27 Behörde, an nachfolgende Kriterien zu knüpfen.
28 Diese sind auch bei einer etwaigen Erweiterung
29 der Kompetenzen in Bezug auf die Quellen-
30 TKÜ auf nicht-polizeiliche Behörden zu beachten:
- 31 • Rechtsgrundlagen für Q-TKÜ sind zu befristen
32 (Ablaufklausel bzw. sunset clause) und
33 müssen nach zwei Jahren durch den Bundes-
34 tag unabhängig evaluiert werden. Sie müssen
35 klar benennen, unter welchen tatbestandlichen
36 Voraussetzungen der Einsatz erlaubt ist.
37 Ein Verweis auf die allgemeinen Aufgaben einer
38 Behörde genügt nicht.
 - 39 • Der Einsatz von Q-TKÜ muss immer einer richterlichen
40 Genehmigung unterliegen (Richtervorbehalt). Dies muss ggf. auch für den Einsatz
41 durch Geheimdienste gelten.
 - 42 • Jeder Einsatz von Q-TKÜ muss im Vorhinein
43 klar befristet und eingegrenzt werden sowie
44 im Anschluss an den Überwachungszeitraum
45 evaluiert werden. Dieser Bericht ist im Falle des
46 Einsatzes durch Geheimdienste dem jeweili-
47

- 48 gen parlamentarischen Kontrollgremium vor-
49 zulegen.
- 50 • Hinweise auf Straftaten, die in keiner Bezie-
51 hung zum Anlass der Q-TKÜ stehen, dürfen nur
52 bei schwersten Straftaten in anderen Verfah-
53 ren weiterverwertet werden, wenn der Einsatz
54 der Q-TKÜ auch in einem Verfahren für diese
55 Straftat erlaubt gewesen wäre (Zufallsfunde).
- 56 • Alle Behörden, die Q-TKÜ durchführen, erstel-
57 len einen jährlichen Bericht, in dem sie klar de-
58 finierte Kennzahlen zu allen Ermittlungsver-
59 fahren, in denen eine Q-TKÜ zum Einsatz kam,
60 offenlegen (mindestens Anzahl der Verfahren
61 mit Q-TKÜ, Dauer der Verfahren sowie Anzahl
62 der Betroffenen und Angaben über Ermitt-
63 lungserfolge). Der Bericht ist im Falle von Ge-
64 heimdiensten dem jeweiligen parlamentari-
65 schen Kontrollgremium vorzulegen und die Öff-
66 fentlichkeit über die Anzahl der Verfahren zu
67 informieren. Berichte der Polizeibehörden sol-
68 len in einer geeigneten Form der Öffentlichkeit
69 zur Verfügung gestellt werden.
- 70 4. Der behördliche Umgang mit IT-Sicherheitslücken,
71 deren Ausnutzung für den Einsatz der Q-TKÜ er-
72 forderlich ist, muss gesetzlich reguliert werden.
73 Ein solches gesetzlich geregeltes Schwachstellen-
74 management muss klare Kriterien für die Risikoab-
75 schätzung im Bezug auf das Geheimhalten von
76 einzelnen Sicherheitslücken beeinhalt, um ein
77 möglichst effektives Schwachstellenmanagement
78 zu garantieren. Ziel muss dabei sein, Sicherheitslü-
79 cken so schnell wie möglich zu schließen.
- 80 5. Die Bundesregierung gibt eine unabhängige Stu-
81 die in Auftrag, die die Zuständigkeiten der deut-
82 schen Sicherheitsbehörden (Geheimdienste und Po-
83 lizei in Bund und Ländern) auf Überschneidungen
84 und Mehrfachzuständigkeiten untersucht. Ziel der
85 Studie ist es, die Zusammenarbeit der Behörden
86 besser zu koordinieren, Doppelarbeit und Kommu-
87 nikationsprobleme zu vermeiden sowie klare Zu-
88 ständigigkeiten zu ermöglichen. Eine solche Entflech-
89 tung schont Ressourcen in den einzelnen Behörden
90 und bündelt alle relevanten Informationen in der je-
91 weils zuständigen Behörde.
- 92 6. Die Bundesregierung beauftragt eine unabhängige
93 wissenschaftliche Studie zur Bestandsaufnahme al-
94 ler Befugnisse und tatsächlichen Maßnahmen, mit-
95 tels derer öffentliche Stellen in die Grundrechte auf
96 informationelle Selbstbestimmung, Vertraulichkeit
97 der Kommunikation sowie auf auf Gewährleistung
98 der Vertraulichkeit und Integrität informationstech-
99 nischer Systeme der Bürger*innen eingreifen oder
100 eingreifen können (sog. Überwachungsgesamtrech-

101 nung). Dies umfasst auch Befugnisse zur Heran-
102 ziehung von Daten privater Stellen. Die Bestands-
103 aufnahme soll jeweils Umfang, Intensität, Dauer
104 und Art der Grundrechtseingriffe sowie die tatsäch-
105 liche Qualität vorgesehener Kontrollmechanismen
106 für diese Eingriffe, insbesondere von Richtervorbe-
107 halten und Datenschutzkontrollen, beinhalten. Die-
108 se sog. Überwachungsgesamtrechnung umfasst so-
109 wohl gezielte als auch ungezielte Befugnisse und
110 Maßnahmen durch öffentliche Stellen, inklusive der
111 Nachrichtendienste, die auf deutschem Staatsge-
112 biet stattfinden oder deutsche Staatsbürger*innen
113 betreffen. Die Studie ist der Öffentlichkeit zur Ver-
114 fügung zu stellen.

115 7. Der bereits beschrittene Weg, die personelle und
116 technische Ausstattung der Polizeibehörden zu ver-
117 bessern wird konsequent weitergeführt. Polizeili-
118 che Ermittlungsarbeit im Internet, wie z.B. die so-
119 genannte "Internetstreife", wird weiter ausgebaut.
120 Ebenso sind Staatsanwaltschaften mit den nötigen
121 personellen und technischen Ressourcen auszustat-
122 ten.

123

124 **Begründung**

125 Mit dem Kabinettsbeschluss vom 21. Oktober 2020
126 will die Bundesregierung den Einsatz von Quellen-
127 Telekommunikationsüberwachung (Q-TKÜ) auf alle
128 Geheimdienste ausweiten. Sie nimmt dabei ohne Not
129 erhebliche Grundrechtseinschränkungen in Kauf und
130 erweist der IT-Sicherheit damit einen Bärendienst.
131 Mittels der sogenannten Q-TKÜ sollen neben Polizeibe-
132 hörden künftig auch die Bundes- und Landesämter für
133 Verfassungsschutz, der Militärische Abschirmdienst und
134 der Bundesnachrichtendienst Zugriff auf Nachrichten und
135 Daten mobiler Messengerdienste erhalten. Dies bedeu-
136 tet in der Praxis, dass Schadsoftware auf Smartphones
137 und Computer aufgespielt wird, um so Daten abziehen.
138 Die neu beschlossenen Befugnisse sollen nicht unter Rich-
139 tertvorbehalt stehen, sondern lediglich von der Zustim-
140 mung der G-10-Kommission abhängen. Eine Überprüfung
141 durch Gerichte ist damit für Betroffene nicht mehr mög-
142 lich. Zudem soll eine Mitwirkungspflicht der Provider ein-
143 geführt werden, um Überwachungssoftware auch vor der
144 Verschlüsselung unbemerkt auf den Endgeräten der Kun-
145 den platzieren zu können. Betroffene werden auch nach
146 Abschluss der Überwachung nicht über den Eingriff infor-
147 miert.

148 Dieses Vorgehen stellt in Anbetracht der Rechtsprechung
149 des Bundesverfassungsgerichts (BVerfG) einen unverhält-
150 nismäßigen Grundrechtseingriff dar. Auch die notwen-
151 dige demokratische Kontrolle und Rechtsschutzmöglich-
152 keiten fehlen. Die Q-TKÜ ist daher entschieden abzuleh-
153 nen. Den Polizeibehörden wurden 2017 bereits weitrei-

154 chende Möglichkeiten zum Einsatz von Überwachungs-
155 software eingeräumt, welche wegen ihrer Tragweite der-
156 zeit auch Gegenstand einer Verfassungsbeschwerde [1]
157 sind. Eine Ausweitung dieser Befugnisse auf Nachrich-
158 tendienste verstößt in ihrer geplanten Form gegen das
159 Trennungsgebot von Polizei und Geheimdiensten. Dies
160 hebt auch der Bundesbeauftragte für den Datenschutz
161 und die Informationsfreiheit Ulrich Kelber in einem State-
162 ment zum Thema [2] hervor. Gleichzeitig können wir be-
163 reits jetzt mit den heute zur Verfügung stehenden Ermitt-
164 lungsmethoden immer häufiger erhebliche Ermittlungs-
165 erfolge von Polizeibehörden im Bereich der Cyberkrimina-
166 lität vermelden, des digitalen Drogenhandels und rechter
167 Chatgruppen. Dringender Bedarf an einer verstärkten Zu-
168 arbeit von mit weitreichenden Kompetenzen weit im Vor-
169 feld von Straftaten ausgestatteten Nachrichtendiensten
170 ohne demokratische und gerichtliche Kontrollmöglichkeit
171 ist nicht erkennbar.

172 Quellen-TKÜ und ähnliche Verfahren bergen ein erhebli-
173 ches Risiko, die IT-Sicherheit in Deutschland und weltweit
174 dauerhaft zu schwächen, da Sicherheitslücken zum Auf-
175 spielen der Staatstrojaner benötigt und bewusst offenge-
176 halten werden. Die beschlossene Mitwirkungspflicht für
177 Telekommunikationsanbieter untergräbt zudem das fun-
178 damentale Vertrauensverhältnis zwischen Internetanbie-
179 ter und Nutzer. Es schädigt die allgemeine IT-Sicherheit
180 zudem noch weiter, da vorgesehen ist, dass Provider die
181 Datenströme unbemerkt umleiten sollen und den Ge-
182 heimdiensten so das Verstecken der Schadsoftware bei-
183 spielsweise in nötigen Sicherheitsupdates ermöglichen.
184 Bürger*innen müssen dadurch fürchten, beim Update
185 ihres Betriebssystems oder ihres Fotobearbeitungspro-
186 gramms Schadsoftware mit herunterzuladen und könn-
187 ten deshalb auf wichtige Updates verzichten (Chilling ef-
188 fect).

189 Dass die Freiheitswahrnehmung der Bürger nicht total
190 erfasst und registriert werden darf, gehört laut Bundes-
191 verfassungsgericht zur verfassungsrechtlichen Identität
192 der Bundesrepublik Deutschland. Der Gesetzgeber ist da-
193 her bei der Erwägung neuer Speicherungspflichten oder
194 -berechtigungen in Blick auf die Gesamtheit der verschie-
195 denen schon vorhandenen Datensammlungen zu Zu-
196 rückhaltung angehalten. Das Bundesverfassungsgericht
197 hat daher mehrfach eine sogenannte "Überwachungsge-
198 samtrechnung" angemahnt. Überwachungsmaßnahmen
199 können einzeln gesehen harmlos wirken und im Einzel-
200 fall gut begründet sein. Ihre Bewertung muss aber im-
201 mer im Kontext aller Überwachungsmöglichkeiten erfol-
202 gen, denn viele Einzelmaßnahmen können in der Über-
203 wachungsgesamtrechnung den Effekt haben, dass Men-
204 schen sich permanent beobachtet fühlen und sich nicht
205 mehr frei äußern (chilling effect).

206 Ebenfalls untersuchen sollte die Bundesregierung, in wie

207 weit Zuständigkeiten in den Sicherheitsbehörden für be-
208 stimmte Deliktsbereiche in zu vielen Behörden gleichzei-
209 tig angesiedelt sind. Allein für die Terrorismusbekämp-
210 fung sind es derzeit etwa 40 verschiedene Behörden [3].
211 Dies verursacht einen immensen Abstimmungsaufwand,
212 birgt die Gefahr von Informationsverlusten und führt zu
213 unklaren Verantwortlichkeiten.
214 Die aufgeführten Maßnahmen sind notwendig, um
215 Grundrechte zu gewährleisten. Wir wollen die Po-
216 lizeibehörden und Staatsanwaltschaften personell
217 und technisch besser ausstatten, um die Sicherheit
218 der Bürger*innen zu gewährleisten. Die derzeit ge-
219 plante Gesetzesänderung stellt hingegen einen mas-
220 siven Einschnitt in die Grundrechte aller Bürger*in-
221 nen dar. Für die Herstellung von Sicherheit darf die
222 Grundrechtsbeschneidung aller aber nicht die Ant-
223 wort sein. [1] <https://freiheitsrechte.org/bka-gesetz/>¹
224 [2] [https://www.bfdi.bund.de/DE/Infothek/Presse-
225 mitteilungen/2020/27_Kritik-TK%C3%9C-2020.html](https://www.bfdi.bund.de/DE/Infothek/Presse-
225 mitteilungen/2020/27_Kritik-TK%C3%9C-2020.html)²
226 [3] [https://www.tagesspiegel.de/themen/agen-
227 da/nach-terror-in-paris-40-behoerden-kooperieren-
228 zur-terrorabwehr-in-deutschland/12628936.html](https://www.tagesspiegel.de/themen/agen-
227 da/nach-terror-in-paris-40-behoerden-kooperieren-
228 zur-terrorabwehr-in-deutschland/12628936.html)³