

Antrag

38. Ordentliche Bundesdelegiertenkonferenz Hamburg, 21. - 23.11.2014

AntragsstellerIn: BAG Medien und Netzpolitik (Beschlossen am 04.10.2014)

Gegenstand: Digitale Selbstbestimmung gewährleisten -
Grenzenlose Überwachung stoppen!

1 Antragstext

2 „Ein Mensch unter Beobachtung ist niemals frei; und eine Gesellschaft unter
3 ständiger Beobachtung ist keine Demokratie mehr.“
4 (SchriftstellerInnen Appell 2013)

5 Seit Juni 2013 werden wir mit immer neuen Enthüllungen zum größten Überwachungs-
6 und Ausspähskandals der Geschichte konfrontiert; kaum fassbare und
7 menschenrechtsverachtende, anlasslose und flächendeckende Überwachungsmaßnahmen
8 werden öffentlich bekannt. Diese Praktiken der Überwachung werden von der
9 amerikanischen NSA oder dem britischen GCHQ oft in Zusammenarbeit mit anderen
10 westlichen Geheimdiensten, inklusive dem deutschen Bundesnachrichtendienst
11 (BND), durchgeführt. Wir GRÜNE fordern ein Ende dieser Totalüberwachung. Daraus
12 folgt eine strikte parlamentarische Kontrolle der Geheimdienste, eine lückenlose
13 Aufklärung über die Zugriffe der Geheimdienste auf personenbezogene Daten im In-
14 und Ausland, zwingend notwendige gesetzliche Klarstellungen bezüglich der
15 Überwachungs-Befugnisse, einen sicheren Aufenthalt für Edward Snowden in
16 Deutschland und Europa und einen besseren gesetzlichen Schutz von
17 Hinweisgeberinnen und Hinweisgebern (Whistleblowern). Darüber hinaus muss die
18 Bundesregierung den verfassungsrechtlich gebotenen Schutz der wichtigsten
19 Kommunikationsinfrastruktur unserer Zeit gewährleisten, um unsere Grund-,
20 Bürger- und Freiheitsrechte, insbesondere das Recht auf Privatsphäre und das
21 Telekommunikationsgeheimnis, auch in der digitalen Welt durchzusetzen. Dies
22 erfordert weitreichende politische und rechtliche Veränderungen, was den
23 rechtlichen und technischen Schutz der Privatsphäre und die Datensicherheit
24 angeht.

25 **Wir GRÜNE fordern daher:**

26 **I. Rechtsstaat und Datensouveränität mit rechtlichen und diplomatischen Mitteln**
27 **verteidigen**

28 **1. Straftaten gegen die Datensouveränität konsequent verfolgen**

29 Straftaten gegen BundesbürgerInnen sind konsequent zu verfolgen - auch und
30 gerade dann, wenn sie von ausländischen Geheimdiensten begangen werden. In den
31 letzten Monaten bekannt gewordene Vorfälle und Programme müssen umfassend
32 untersucht, der Sachverhalt vollständig ausermittelt und, wo möglich, den
33 deutschen Gerichten zugeführt werden. Die entsprechend verantwortlichen Personen
34 in Deutschland sind zu identifizieren und strafrechtlich zu verfolgen oder,
35 falls sie diplomatischen Schutz genießen, entweder auszuweisen oder zur
36 unerwünschten Person zu erklären. Gegen EU-Mitgliedsstaaten, deren Geheimdienste
37 weiterhin Angriffe auf Informationssysteme anderer Mitgliedsstaaten unternehmen,
38 muss ein Vertragsverletzungsverfahren angestrengt werden. Deutsche
39 Ermittlungsbehörden sollten zur Aufdeckung der in Deutschland stattgefundenen
40 Angriffe alle notwendigen Ressourcen einsetzen, insbesondere die Unterstützung
41 des Cybercrime Center von Europol für entsprechende Ermittlungen anfordern, da
42 dies nicht eigeninitiativ tätig werden darf.

43 **2. Keine Duldung von und Kooperation mit rechtsverletzenden ausländischen**
44 **Geheimdiensten**

45 Jede Form der Duldung von und Kooperation deutscher Behörden mit ausländischen
46 Geheimdiensten, die offensichtlich rechtswidrig BürgerInnen in Deutschland
47 überwachen, muss umgehend eingestellt werden. Insbesondere dürfen die deutschen
48 Geheimdienste nicht mit ausländischen Diensten Daten austauschen bzw. deren
49 Datenerhebung im Inland unterstützen, wenn die ausländischen Dienste die Daten
50 auf nicht nachweisbaren oder gesetzeswidrigem Weg erlangten und/oder sie einer
51 Nutzung zuführen, die für deutsche Dienste verboten ist. Die Verhinderung der
52 großflächigen Ausforschung von BürgerInnen in Deutschland muss von den deutschen
53 Diensten als Teil der Spionageabwehr verstanden werden; entsprechende Methoden
54 und Ressourcen sind einzusetzen. Die Kooperation mit anderen Geheimdiensten, z.
55 B. über das EU-Intelligence Center (INTCENT), muss eingestellt werden, solange
56 diese keine Rechtsgrundlage im EU-Recht hat und keine angemessenen rechtlichen
57 Rahmenbedingungen und Praktiken der kooperierenden Geheimdienste vorliegen. Die
58 Bundesregierung und die Europäische Kommission müssen sicherstellen, dass sich
59 ausnahmslos alle EU-Mitgliedsstaaten und ihre Geheimdienste an geltende
60 nationale und europäische (grund-)rechtliche Vorgaben halten. Wir brauchen
61 unverzüglich europaweite und langfristig weltweite Mindeststandards für
62 geheimdienstliche Eingriffe in Grundrechte und ein effektives Kontroll- und
63 Sanktionsregime.

64 **3. Informationelle Selbstbestimmung der BürgerInnen als Voraussetzung**
65 **internationaler Zusammenarbeit**

66 Unser Recht auf Privatheit und unsere Datensouveränität, das haben die
67 Enthüllungen Edward Snowdens gezeigt, stehen derzeit massiv in Frage. Es ist
68 gegen staatliche und nichtstaatliche Akteure, egal ob diese inner- oder
69 außerhalb der EU beheimatet sind, mit allen zur Verfügung stehenden Mitteln zu
70 verteidigen. Die Bundesregierung muss unmissverständlich deutlich machen, dass
71 sie die Verletzung der Privatsphäre ihrer BürgerInnen nicht hinnimmt und hierauf
72 entsprechend reagiert. Insbesondere sollte die Bundesregierung die
73 vollumfängliche Beachtung der - auch verfassungsrechtlich gebotenen -

74 Datensouveränität von BürgerInnen und Unternehmen zur Mindestbedingung von
75 Zusammenarbeit machen, z. B. in Bezug auf die Bereitschaft zum Datenaustausch
76 bei Sicherheitspartnerschaften, Freihandelsabkommen oder der Vergabe von
77 öffentlichen Aufträgen. Der Abschluss eines Rahmenabkommens zum Datenschutz im
78 Strafverfolgungsbereich zwischen der EU und den USA mit effektiven,
79 durchsetzbaren Rechten für europäische BürgerInnen muss Bedingung für jede
80 weitere Zusammenarbeit mit US-Behörden sein. Bestehende Datenaustauschabkommen,
81 zum Beispiel bezüglich des Austauschs von Bank- oder Fluggastdaten, müssen vor
82 dem Hintergrund der Erkenntnisse der letzten Monate aufgekündigt werden.

83 **4. Deutsche Geheimdienste demokratisch einhegen und kontrollieren**

84 Auch die Befugnisse der deutschen Geheimdienste und Sicherheitsbehörden sind,
85 das hat eine entsprechende Anhörung namhafter Verfassungsrechtler des
86 Parlamentarischen Untersuchungsausschuss des Deutschen Bundestages deutlich
87 gemacht, gesetzlich einzuhegen und die praktische Umsetzung sehr viel effektiver
88 zu kontrollieren, allen voran durch die Parlamente, in den Diensten selber,
89 durch die Gesellschaft und die Judikative. Die Möglichkeiten der technischen
90 Überwachung müssen klar eingegrenzt werden. Bekannt gewordene Praktiken, vor
91 allem was den Einsatz gemeinsamer Programme mit ausländischen Diensten und
92 offenbar gewordenen Ringtausch-System von rechtswidrig erlangten Daten angehen,
93 sind mit verfassungsrechtlichen Vorgaben nicht zu vereinbaren und müssen daher
94 umgehend eingestellt werden. Das bewusste Verbauen und Offenhalten von
95 Sicherheitslücken und die Kompromittierung von Netzinfrastrukturen und
96 Computern, sind zu untersagen..) Auch im Ausland dürfen grundsätzlich durch
97 deutsche Dienste keine Praktiken eingesetzt werden, die im Inland verboten sind.
98 Die parlamentarischen Kontrollgremien sind besser auszustatten und mit
99 robusteren und konkreteren Befugnissen zu versehen. Die Information muss
100 zukünftig umfassend und proaktiv, nicht bloß wie bisher unvollständig und nur
101 auf direkte Nachfrage erfolgen. Die Transparenz und die
102 Rechtsschutzmöglichkeiten von Betroffenen sind zu verbessern. Whistleblower
103 verdienen effektiven rechtlichen Schutz, besonders, wenn sie Informationen
104 offenlegen, die klar rechtswidriges Handeln bspw. von in- oder ausländischen
105 staatlichen Behörden betreffen. Sowohl der NSU- als auch der NSA-Skandal haben
106 ein mannigfaltiges Versagen der Dienste offenbart. Hieraus müssen wir
107 Konsequenzen ziehen: Für das Bundesamt für Verfassungsschutz fordern wir eine
108 vorübergehende Auflösung und eine anschließende Debatte, welche Kompetenzen in
109 einer neu zu gründenden Stelle wie fortgeführt werden könnten. Den Militärischen
110 Abschirmdienst (MAD) wollen wir abwickeln.

111 **5. Unabhängigkeit der Institutionen**

112 Die Bundesregierung wird endlich einen ersten wichtigen Schritt gehen, und die
113 Bundesbeauftragte für Datenschutz und Informationsfreiheit aus der direkten
114 Verantwortlichkeit des Bundesinnenministeriums herauslösen. Damit setzt sie die
115 seit Jahren überfällige Unabhängigkeit, die von uns gemeinsam mit dem
116 Europäischen Gerichtshof wiederholt eingefordert wurde, endlich um. Nun muss
117 dringend eine den aktuellen Herausforderungen angemessene personelle und
118 finanzielle Ausstattung beschlossen werden. Ein ähnlicher Schritt steht beim
119 Bundesamt für Informationssicherheit (BSI) noch aus. Wir wollen auch dieses
120 Bundesamt unabhängig vom Innenministerium stellen. Durch erweiterte Befugnisse
121 und eine verbesserte personelle und finanzielle Ausstattung wollen wir
122 sicherstellen, dass das Amt zukünftig den in den letzten Jahren massiv
123 gestiegenen Herausforderungen gerecht werden und seine vielfältigen Aufgaben in

124 angemessener Art und Weise wahrnehmen kann. Bisher weigert sich die
125 Bundesregierung, diese Vorschläge umzusetzen.

126 II. Technische Datensicherheit in den Kern der politischen Gestaltung rücken

127 **1. Staatliche Unterstützung für sichere Informationstechnik**

128 Sowohl bei der Vergabe öffentlicher Aufträge als auch bei der staatlichen
129 Forschungspolitik muss zukünftig ein Schwerpunkt auf die Entwicklung und
130 Förderung sicherer - möglichst freier - Software gelegt werden. Bekannte
131 Sicherheitsvorfälle bei Unternehmen sind als negative Bewertung bei der
132 öffentlichen Beschaffung zwingend zu berücksichtigen. Das erfordert ein
133 radikales Umdenken, denn statt durch Förderprogramme wie INDECT Unsicherheit und
134 Überwachung finanziell zu unterstützen, muss der Fokus auf Landes-, Bundes- und
135 Europaebene zukünftig auf der Förderung sicherer Technik liegen.
136 Dementsprechend ist es wichtig, einerseits die IT- und Datensicherheitsforschung
137 im Rahmen staatlicher Institutionen zu fördern und in diese zu investieren,
138 andererseits aber auch Anreize für unabhängige Sicherheitsforschung zu schaffen,
139 ihre Erkenntnisse zur Verbesserung der Sicherheit aller einzusetzen. Diese
140 Schwerpunktsetzung kann somit auch zur Veröffentlichung von Sicherheitslücken
141 gegen den Wunsch des Herstellers führen.
142 Ein besonderer Schwerpunkt muss die Entwicklung und Verbreitung ebenso robuster
143 wie benutzerfreundlicher Cryptosysteme bilden. Hier ist der Aufholbedarf groß.
144 Der Staat soll in entsprechende Forschung und Ausbildung investieren, denn
145 hierbei handelt es sich im wahrsten Sinne des Wortes um eine
146 Schlüsseltechnologie im digitalen Raum. Wir brauchen endlich durchgehende Ende-
147 zu-Ende-Verschlüsselung bei allen IT-Großprojekten. Nur so ist in den letzten
148 Monaten massiv verloren gegangenes NutzerInnen-Vertrauen in die globale
149 Internetinfrastruktur langfristig zurückzugewinnen und Datensouveränität
150 effektiv zu gewährleisten. Gerade in diesem Bereich sollte darüber nachgedacht
151 werden, gezielte Förderprogramme für freie und offene Software zu entwickeln, um
152 die Nachprüfbarkeit des Quellcodes, die Weiterentwicklung und -nutzbarkeit von
153 Produkten zu sichern.

154 Langfristige Forschungsschwerpunkte sollten auch auf "Software-Verifikation"
155 liegen und eine Offensive für hier vor Ort entwickelte und produzierte
156 Technologie angestrebt werden (z. B. in der Chip-, Netzwerk- und
157 Speichertechnik). Deutschland sollte hier - auch vor dem Hintergrund des hohen
158 deutschen Datenschutzniveaus - innerhalb Europas eine Vorreiterrolle einnehmen.
159 Zwingend einhergehen muss dies mit dem klaren gesetzlichen Verbot an
160 Geheimdienste und andere Sicherheitsbehörden, Einfluss auf die Forschung und
161 Entwicklung solcher Technik zu nehmen. Deutsche und europäische
162 Ausschreibungsbestimmungen müssen überprüfbar sichere IT beinhalten, etwa durch
163 Bevorzugung von Open-Source-Lösungen.

164 **2. Einführung einer gesetzlichen Pflicht, Sicherheitslücken umgehend zu beheben**

165 Es bedarf einer umfassenden Meldepflicht für Sicherheitsvorfälle im IT-Bereich.
166 Zudem bedarf es einer Verbesserung der Überprüfbarkeit von Software durch den
167 Zwang, anders als bisher mit Sicherheitsproblemen umzugehen. Es muss eine
168 gesetzliche Verpflichtung geben, Schwachstellen umgehend zu melden und
169 schnellstmöglich zu beheben. Im Bereich offener Software sollte der Staat
170 Systeme zur schnellen Behebung fördern und eine öffentlich einsehbare Warnliste

171 mit entsprechend bekannten Problemen pflegen. Außerdem treten wir für Änderungen
172 der Haftungs- und Gewährleistungsregeln ein, um Unsicherheit signifikant teurer
173 zu machen als Untätigkeit. Die Haftung sollte für Herstellung und Vertrieb von
174 Software gelten, die nicht auf quelloffener Software basiert. Dabei sollten
175 nicht die Schwachstellen selbst zu einer Sanktion führen, sondern nur der
176 falsche Umgang mit Sicherheitsproblemen. Voraussetzung der Haftung für
177 Sicherheitslücken sollte sein, dass diese trotz Kenntnis des Verantwortlichen
178 nicht in angemessener Zeit gemeldet und geschlossen worden sind.
179 Die Meldepflichten im geplanten IT-Sicherheitsgesetz und in der sich kurz vor
180 dem Abschluss befindlichen Netzwerk- und Informationssicherheits-Richtlinie der
181 EU sind ein Schritt in die richtige Richtung, greifen aber zu kurz, weil sie nur
182 neue Sicherheitsvorfälle adressieren, darüber hinaus aber keine Regeln zum
183 Umgang mit bekannten Schwachstellen enthalten. Zudem sollen sie nur für
184 Unternehmen, nicht jedoch für staatliche Stellen gelten. Die Bundesregierung
185 muss sich bei ihrem eigenen Gesetz und im Ministerrat für die europäische
186 Richtlinie dafür einsetzen, dass auch bekannt gewordene Schwachstellen
187 angegangen und auch staatliche Stellen zur Meldung und Schließung von Lücken
188 verpflichtet werden.
189 Eine besondere Verpflichtung haben die Zertifizierungsstellen (Certificate
190 Authorities, CA). Sie sind für das Erstellen, die Ausgabe, Verwaltung und
191 Sperrung von digitalen Zertifikaten zuständig. Werden von ihnen technische
192 Schwachstellen bewusst verschwiegen und nicht umgehend behoben und nach deren
193 Beseitigung öffentlich gemacht, so muss neben empfindlichen Geldstrafen auch die
194 Möglichkeit weiterer, effektiver Sanktionen wie dem Strafrecht bestehen.

195 **3. Gesetzliche Gewährleistung des Rechts, Unsicherheit thematisieren zu dürfen**
196 Wir wollen das Aufdecken technischer Schwachstellen fördern. Wer
197 Sicherheitslücken aufdeckt, den Hersteller informiert und ihm eine angemessene
198 Zeit zur Korrektur einräumt, bis er die Sicherheitslücke veröffentlicht (sog.
199 Responsible Disclosure), darf hierfür nicht bestraft oder kriminalisiert werden.
200 Es muss vielmehr Unterstützung und Anreize geben, technische Unsicherheit
201 aufzudecken und klar zu benennen, um mögliche Schäden so klein wie möglich zu
202 halten. Um dieses Ziel zu erreichen, darf es kein generelles Verbot von
203 Hackertools geben. Wir wollen außerdem keine Kriminalisierung des umfassenden
204 Aufdeckens von Sicherheitslücken (Full-Disclosure-Ansatz). Entscheidend ist die
205 Differenzierung bei der Ausnutzung dieses Wissens, das heißt zu unterscheiden,
206 ob es z. B. zur Schädigung Dritter genutzt wird oder es legitimer
207 Sicherheitsforschung dient.

208 **4. Mitwirkung staatlicher Stellen bei der Gewährleistung von IT-Sicherheit**
209 Es muss staatlichen Stellen untersagt sein, die Sicherheit und Integrität von
210 IT-Produkten und der Kommunikationsinfrastruktur negativ zu beeinflussen.
211 Keinesfalls dürfen staatliche Institutionen und insbesondere Geheimdienste den
212 Schwarzmarkt für Sicherheitslücken befördern, indem sie dort als Käufer oder
213 Verkäufer auftreten. Vielmehr muss gelten: Sobald eine staatliche Institution
214 Kenntnis von einer Sicherheitslücke erlangt, muss sie verpflichtet sein, diese
215 schnellstmöglich zu melden und zu ihrer Beseitigung beizutragen. Das heißt, den
216 Hersteller in Kenntnis zu setzen, auf die Beseitigung der Sicherheitslücke zu
217 drängen, ggf. auch die Öffentlichkeit zu warnen und bei offener Software mit
218 ihren Möglichkeiten zu unterstützen, die Schwachstellen zu beheben.

219 **5. Einzelne NutzerInnen stärken**

220 Wir sagen klar: Die bekannt gewordenen Praktiken verschiedener westlicher
221 Geheimdienste, die eng mit großen IT-Firmen kooperieren und unsere Rechner und
222 Kommunikationsinfrastruktur weitreichend kompromittiert haben, müssen vor allem
223 tiefgreifende gesetzgeberische Konsequenzen mit dem Ziel der Wiederherstellung
224 der Herrschaft des Rechts nach sich ziehen. Gleichzeitig kann ein effektiver
225 Schutz der eigenen Daten und IT Struktur ein Baustein sein, die eigene
226 Datensouveränität zu stärken. Neben der staatlichen Unterstützung für eine
227 sichere technische Software- und Hardwareinfrastruktur muss es auch Wege zur
228 Stärkung der einzelnen NutzerInnen geben. Dazu gehören beispielsweise ein
229 effektives modernisiertes Datenschutzrecht, der Schutz und der Ausbau der
230 informationellen Selbstbestimmung, eine den Herausforderungen angemessen
231 ausgestattete Datenschutzaufsicht sowie der Ausbau entsprechender
232 Bildungsangebote auf allen Ebenen wie auch weitreichende Auskunftsrechte für die
233 Betroffenen. Eine Nutzung von Internetdiensten und Telemedienangeboten unter
234 Pseudonymen oder anonym muss weiterhin möglich sein. Wir wollen die
235 informationelle Selbstbestimmung auch dadurch stärken, dass Datenhehlerei als
236 Straftatbestand eingeführt wird. Um europaweit einen starken Datenschutz mit
237 echten Durchsetzungsmöglichkeiten zu bekommen, muss das Bundesinnenministerium
238 sich endlich konstruktiv und ergebnisorientiert an den Verhandlungen zur EU-
239 Datenschutz-Grundverordnung beteiligen.

240 **Debatte vorantreiben**

241 Die Digitalisierung aller Lebensbereiche geht einher mit einer zunehmenden
242 Automatisierung. Diese Entwicklungen schreiten voran und haben weitreichende
243 Auswirkungen auf unsere informationelle Selbstbestimmung aber auch auf unsere
244 Arbeitswelt, unser soziales Zusammenleben, unsere Wirtschaft und unser
245 Alltagsleben. Wir Grüne stehen dabei an vielen Stellen vor zahlreichen neuen
246 Herausforderungen und vor Fragen auf die wir noch keine abschließenden Antworten
247 haben. Um den Diskussionsprozess über diese Entwicklungen voranzutreiben und
248 Antworten zu erarbeiten, wird der Bundesvorstand gebeten im Jahr 2015 in
249 Zusammenarbeit mit den Bundesarbeitsgemeinschaften eine eigenständige
250 inhaltliche Veranstaltung dazu zu organisieren.

Begründung

mündlich