

## V-01 Verschiedenes

Antragsteller\*in: Malte Spitz (Parteirat)

### „Datenschutz ist der neue Umweltschutz“

- 1 „Datenschutz ist der neue Umweltschutz“
- 2 Informationelle Selbstbestimmung ist ein Grundrecht und essentiell, um die Privatsphäre und
- 3 die Entfaltung jedes Menschen zu schützen und zu ermöglichen. Trotzdem wird gerade aus
- 4 Reihen der Bundesregierung immer wieder der Datenschutz offen in Frage gestellt und ein
- 5 vermeintlicher Gegensatz von Datenschutz und wirtschaftlicher Entwicklung konstruiert. Zudem
- 6 wird der Schutz persönlicher Daten als Hemmnis einer guten Sicherheitspolitik dargestellt.
- 7 Dies erleben wir gerade dieser Tage. Das Schema ist ein altbekanntes: Ein terroristischer
- 8 Anschlag wird genutzt, um an der Sicherheitsschraube zu drehen und unseren Rechtsstaat
- 9 konstituierende Freiheitsrechte offen in Frage zu stellen. Wenn der für den Schutz unserer
- 10 Verfassung zuständige Minister zu Protokoll gibt, dass Datenschutz schön sei, aber in
- 11 Krisenzeiten und darüber hinaus Sicherheit Vorrang habe, offenbart dies ein krudes
- 12 Rechtsstaatsverständnis, dem wir uns als Grüne entschlossen entgegenstellen.
- 13 Wer, um von eigenen Versäumnissen der letzten Monate abzulenken, Freiheits- und Grundrechte
- 14 wie den Datenschutz offen in Frage stellt, hat nicht ansatzweise verstanden, worum es den
- 15 Terrorist\*innen geht, nämlich darum, unsere Gesellschaft zu spalten und die Freiheit und
- 16 Offenheit unserer Demokratien anzugreifen. Die Antwort auf Hass und Terror kann und darf
- 17 daher niemals Demokratieabbau und Krieg, sondern nur noch mehr Rechtsstaatlichkeit,
- 18 Entschlossenheit, Freiheit und Toleranz sein.
- 19 Der Datenschutz - in der digitalen Realität unserer von Algorithmen zunehmend geprägten
- 20 Gesellschaft ein noch essentielleres Freiheitsrecht denn je - schützt den/die EinzelneN vor
- 21 unternehmerischer und staatlicher Ausspähung. Ein Hindernis für eine effektive
- 22 Sicherheitspolitik ist er, zumindest in demokratischen Rechtsstaaten, nicht. Stattdessen
- 23 stellen verlässliche und hohe, einheitliche Datenschutzstandards die Voraussetzung für eine
- 24 gute und akzeptierte Arbeit von Polizei und Sicherheitsbehörden dar. Es ist nötig, endlich
- 25 die zielgerichtete Verfolgung von Terrorverdächtigen zu verbessern und dafür mehr Personal
- 26 bereitzustellen.
- 27 Die Bundesregierung hat noch immer nicht erkannt, dass anlasslose Datensammlungen, erhoben
- 28 etwas im Rahmen von Vorratsdatenspeicherungen, durch Bankdatenabgleiche oder durch
- 29 Flugpassagierüberwachungen, nicht dazu geführt haben, die Sicherheit vor Anschlägen zu
- 30 erhöhen, im Gegenteil: Die Suche nach der Nadel im Heuhaufen, das ist eine bittere Erfahrung
- 31 aus den Anschlägen von Paris und Brüssel, wird für die Ermittler\*innen immer schwieriger,
- 32 die Lage in einem Meer aus Information immer unübersichtlicher.
- 33 Längst haben höchste Gerichte dieser Praxis präventiver, unserer Rechtsordnung fremder,
- 34 anlassloser Datenspeicherungen mit Hinweis auf deren Unvereinbarkeit mit geltenden
- 35 Grundrechten eine klare Absage erteilt. So ist die Rechtsprechung längst zu einem Korrektiv
- 36 einer grundrechtsgefährdenden weil oft unverhältnismäßig agierenden Gesetzgebung der Großen
- 37 Koalition geworden. Dabei wäre es ihre originäre Aufgabe, den Grundrechtsschutz zu
- 38 gewährleisten und angesichts der massiven Bedrohungen der informationellen Selbstbestimmung
- 39 rechtliche Sicherungsmechanismen wie beispielsweise den Art. 10 GG auszubauen. Dies würde

40 nicht nur zu einem höheren Grundrechtsschutz der Bürger\*Innen, sondern auch zu mehr Daten-  
41 und Rechtssicherheit für die Unternehmen führen.

#### 42 **Datenschutz made in Germany**

43 Datenschutz und wirtschaftlicher Erfolg sind keineswegs Gegensätze. Datenschutz und  
44 Datensicherheit sind für die große Mehrheit der Unternehmen vielmehr von essentieller  
45 Bedeutung und eine Zukunftschance für hiesige Unternehmen, die auf ein großes Know-How von  
46 IT-Sicherheitslösungen made in Germany zurückgreifen können. Mit Ausnahme der wenigen  
47 internationalen Akteure, die mit unseren Daten unvorstellbar viel Geld verdienen, wird das  
48 Fehlen von Rechtssicherheit und Standards ganz überwiegend als Hemmnis der wirtschaftlichen  
49 Entwicklung wahrgenommen.

50 Mehr noch: Datenschutz und Datensicherheit können eine, das haben die letzten Monate  
51 eindrucksvoll gezeigt, sehr erfolgsversprechende Wirtschaftsstrategie sein. Selbst große US-  
52 Konzerne haben zuletzt die marktstrategische Bedeutung von IT-Sicherheit und dem Schutz  
53 persönlicher Daten erkannt. Sie verlegen ihre Rechenzentren auf den Europäischen Kontinent  
54 und wehren sich öffentlichkeitswirksam gegen die staatliche angeordnete Entschlüsselung von  
55 Mobiltelefonen in den USA. Der Grund ist sehr einfach: Vertrauen ist nicht nur gut für die  
56 Akzeptanz neuer, digitaler Angebote, sondern auch gut für Geschäfte. Dieses Vertrauen  
57 besteht in den USA aufgrund der Enthüllungen Snowdens und Verpflichtungen aufgrund von  
58 intransparenten Entscheidungen von Geheimgerichten nicht mehr. In Deutschland gehören  
59 durchgehende Ende-zu-Ende-Verschlüsselung noch immer nicht zum Standard bei großen IT-  
60 Projekten. Hierfür haben wir uns als Grüne immer wieder eingesetzt und auf die Bedeutung  
61 vertraulicher Kommunikation hingewiesen. Einige Unternehmen haben die Bedeutung sicherer  
62 Verschlüsselungslösungen mittlerweile, anders als die Bundesregierung, erkannt und werben  
63 offensiv mit einer „Cloud made in Germany“. Diese Beispiele zeigen, dass wir in unserem  
64 Ringen nach mehr Datenschutz und Datensicherheit immer mehr Verbündete haben. Noch wichtiger  
65 ist die Erkenntnis, dass Deutschland und Europa tatsächlich relevante Standards setzen und  
66 diese zukünftig hoffentlich auch durchsetzen können. Wir sollten daher Datenschutz und  
67 Datensicherheit zu einem Markenkern unseres Wirtschaftsstandorts machen. Hierfür bedarf es  
68 neben einer Stärkung bestehender Aufsichtsstrukturen, einer größeren Unterstützung der  
69 wichtigen Arbeit der Verbraucherzentralen auch der Unabhängigkeit des noch immer dem  
70 Bundesinnenministerium unterstellten Bundesamt für Sicherheit in der Informationstechnik.

71 Zudem brauchen wir eine anpackende Umsetzung der EU-Datenschutzreform in bundesdeutsches  
72 Recht samt Nutzung bestehender Gestaltungsspielräume, beispielweise bezüglich eines  
73 effektiven Beschäftigtendatenschutzes. Hier liegt eine wahre Mammutaufgabe vor uns. Genauso  
74 müssen wir bestehende wettbewerbs-, kartell- und fusionsrechtliche Regelungen dahingehend  
75 weiterentwickeln, dass zukünftig die Rolle monopolartiger Anbieter mit extrem hohen  
76 Datenkonzentrationen stärker berücksichtigt wird.

77 Wir treten weiterhin für hohe Datenschutzstandards beim Datenaustausch mit Drittstaaten ein,  
78 die auch tatsächlich als Rechte ausgestaltet sind. Unser Verständnis des Datenschutzes als  
79 Grundrecht muss auch in diesen Abkommen zum Ausdruck kommen. Das hat zuletzt der Europäische  
80 Gerichtshof in seinem Urteil zum „Safe Harbor“-Abkommen unmissverständlich klargemacht. Das  
81 Urteil war nicht nur wie bereits zuvor das Urteil zur EU-Vorratsdatenspeicherungs-Richtlinie  
82 eine weitere wichtige Grundsatzentscheidung. Das Urteil war auch eine schallende Ohrfeige  
83 für die Bundesregierung, die, trotz des Umstandes, dass wir immer wieder vor genau dieser  
84 Entwicklung gewarnt haben, bis zuletzt an dem klar rechtswidrigen Abkommen festgehalten hat.  
85 Die nach dem Urteil des höchsten europäischen Gerichts entstandene Rechtssicherheit geht  
86 somit voll auf ihr Konto. Sollte das nun vorgelegte „Privacy Shield“ erneut vom EuGH  
87 kassiert werden, hat sie die erneut entstehende Rechtsunsicherheit zu verantworten.

#### 88 **Mit Datenschutz schwarze Zahlen schreiben**

89 Schon jetzt werden von europäischen Unternehmen mit Soft- und Hardware basierter  
90 Sicherheitstechnik Milliarden umgesetzt. Diese Technik dient auch dem Schutz der Daten der  
91 Verbraucher\*innen und Verbraucher bei der Verwendung vernetzter Geräte und wird in diesem  
92 Sinne beworben. Wir sind überzeugt, dass wie bei den Umwelttechnologien auch Produkte, die  
93 Datenschutz und Datensicherheit in besonderer Weise gewährleisten, Exportschlager sein  
94 können. Das bedeutet, dass wir den Mittelstand in punkto IT-Sicherheit voranbringen und  
95 damit zukunftsfähig machen müssen. Auch Startups, die bewusst in entsprechende Lösungen  
96 investieren, müssen sehr viel stärker unterstützt werden als bisher.

97 Wir wollen die rechtlichen Rahmenbedingungen so gestalten, dass Verbraucher\*Innen in die  
98 Lage versetzt werden, bewusste Kaufentscheidungen zu treffen und so datenschutzkonforme und  
99 -sichere Produkte auszuwählen. Hierfür ist es von Nöten, mehr Transparenz, beispielsweise  
100 bezüglich eingesetzter Algorithmen, zu schaffen. Angelehnt an die Energieeffizienzklassen  
101 von Haushaltsgeräten soll eine entsprechende Klassifizierung oder auch Zertifizierung für  
102 vernetzte Haushaltsgeräte, Fahrzeuge etc. eingeführt werden.

103 Das Recht auf Verschlüsselung sowie ein Recht auf Anonymisierung ohne Hintertüren muss  
104 dauerhaft gesichert und ausgebaut werden. Diese Standortvorteile gegenüber USA gilt es zu  
105 bewahren und festzuschreiben, auch und gerade gegenüber staatlichen Stellen. Klare  
106 Zugriffsbeschränkungen deutscher Nachrichtendienste sind zwingend eindeutig zu definieren  
107 und effektiv zu kontrollieren. Wir setzen uns zudem für eine verfassungsrechtliche Einhegung  
108 der Befugnisse der Dienste sowie eine komplette Neuaufstellung der Aufsicht  
109 geheimdienstlicher Tätigkeit ein.

110 Wir halten zudem ein staatlich finanziertes Programm zur Beratung bei der IT-Sicherheit für  
111 kleinere und mittlere Unternehmen (KMUs) für notwendig. Auch hier bieten die Erfahrungen des  
112 Umweltschutzes mit der Energieberatung gute Anknüpfungspunkte für die weitere Ausgestaltung.  
113 Sicherheitsberatung in die Fläche zu bringen, erhöht nicht nur den Schutz für die  
114 Unternehmen, sondern schützt vor allem die Daten der Millionen Kund\*Innen, die bei diesen  
115 Unternehmen vorliegen. Mit diesem dezentralen Netz an IT-Sicherheitsberater\*Innen kann auch  
116 eine erste Aufklärung über Digitalisierung, Automatisierung und Vernetzung in den KMUs  
117 stattfinden, und damit das notwendige Umdenken und Überdenken anstoßen.

### 118 **Datenschutz sichert die Ressource Freiheit**

119 Neben einer lebenslang vermittelten Medienkompetenz, sind Datensouveränität und  
120 Datensicherheit heute wesentliche Bedingungen für ein freies und selbstbestimmtes Leben. Je  
121 mehr der Staat oder Unternehmen über mich wissen, desto unfreier werde ich. Ich verhalte  
122 mich anders, wenn ich weiß, dass ich beobachtet werde und Spuren hinterlasse, über die ich  
123 keine Kontrolle mehr habe. In einer solchen Situation passen wir uns alle an. Die Schere im  
124 Kopf entsteht. Das ist Gift für die Demokratie. Freiheitliche Gesellschaften brauchen  
125 Freiräume, in den sich die Bürger\*Innen unbeobachtet ausprobieren und entfalten können. Es  
126 ist nicht nur für jeden schön, auch Geheimnisse haben zu können - für bestimmte Gruppen wie  
127 Journalist\*Innen, Ärzt\*Innen, Rechtsanwält\*Innen und Seelsorger\*Innen ist es sogar  
128 essentiell. Eine geschützte Kommunikation muss daher nicht nur Ihnen zwingend ermöglicht und  
129 ausgebaut werden.

130 Der Staat und einige Unternehmen betreiben daher mit ihrer Datensammelwut Raubbau an der  
131 Ressource Freiheit. Und wie beim Umweltschutz können wir Fehlentwicklungen im Nachhinein  
132 nicht oder nur mit sehr viel größeren Aufwand reparieren. Der „Point-of-no-return“, die  
133 digitale 2-Grad-Grenze naht: Denn wenn meine Daten erst einmal in den Datenbanken großer  
134 Unternehmen und (fremder) Staaten gespeichert, gerastert und zu höchst aussagekräftigen  
135 Profilen verknüpft sind, haben wir die Kontrolle hierüber bereits verloren. Daher müssen wir  
136 jetzt handeln und den immer weiter ausufernden Datensammlungen und einer weitreichenden  
137 Spionage klare rechtliche Grenzen setzen. Die Politik darf den technischen Möglichkeiten und

138 den durch sie entstehenden Gefahren für den Grundrechtsschutz nicht länger hinterherlaufen,  
139 sondern muss die Digitalisierung und den Schutz privater Kommunikation und  
140 Geschäftsgeheimnissen als vordringliche Herausforderung annehmen.

141 Als Bürgerrechtspartei liegt es auch in der besonderen Verantwortung der Grünen, die  
142 Bedeutung eines innovativen Datenschutzes als Grundlage für ein selbstbestimmtes Leben auch  
143 und gerade in der digitalen Welt immer wieder zu betonen.

#### 144 **Grundrechte in der digitalen Welt stärken**

145 Wie nötig aber auch der Ausbau bestehender Mechanismen zum Schutz vor unternehmerischer und  
146 geheimdienstlicher Ausspähung ist, halten uns anhaltende Datenskandale, IT-Angriffe auf den  
147 Deutschen Bundestag und andere Institutionen und nicht zuletzt die anhaltenden Enthüllungen  
148 des Whistleblowers Edward Snowden vor Augen.

149 Der Datenschutz ist es, der einem totalitären Anspruch datensammelnder Unternehmen und  
150 Geheimdienste einen Riegel vorschiebt und verhindert, dass auch der letzte Teil unserer  
151 Privatsphäre verdatet wird. Er verhindert, dass unser aller Leben bis in den letzten Winkel  
152 überwacht, gerastert und profiliert wird. Längst geht es nicht mehr um einzelne Datensätze,  
153 sondern um die Zusammenführung und systematische Analyse aller vorhandenen Daten und  
154 Informationen. Aktuell befinden sich diese Daten oftmals noch verteilt in unterschiedlichen  
155 Datenbanken rund um den Globus. Immer öfter werden sie jedoch von Unternehmen verknüpft und  
156 gerastert. Und staatliche Stellen, das ist die Erkenntnis nach gut zwei Jahren Aufklärung im  
157 Untersuchungsausschuss des Bundestags zur geheimdienstlichen Praxis von NSA und BND,  
158 verschaffen sich auf legalem oder illegalem Weg Zugriff auf sie.

159 Die skizzierten technologischen Entwicklungen werden uns absehbar auch die kommenden  
160 Jahrzehnte begleiten. Die digitalen Datenmengen, die wir produzieren, verdoppeln sich in  
161 immer kürzeren Intervallen. Und mit ihnen steigen auch die Begehrlichkeiten, an diese  
162 Datenberge heranzukommen, sie zu vermarkten, zu rastern, zu Profilen zu verknüpfen und uns  
163 alle in ein digitales Kastensystem einzusortieren, das im offenen und klaren Widerspruch zu  
164 bestehenden Solidarsystemen steht.

165 Als Grüne werden wir nicht müde auf diese Gefahren für die informationelle Selbstbestimmung  
166 der Menschen hinzuweisen. Wir werden nicht müde, die Bundesregierung aufzufordern, sich,  
167 statt den Datenschutz in Frage zu stellen, auch endlich an den für die digitale Gesellschaft  
168 so wichtigen Fragestellungen angemessen zu beteiligen.

169 Auch die Bundesregierung muss sich fragen, ob bestimmte Geschäftsmodelle mit der  
170 Menschenwürde vereinbar sind, und ob es nicht Grenzen der Überwachung und Ausforschung, und  
171 der Algorithmisierung ganzer Lebensbereiche geben muss. Darüber, ob man monopolartige  
172 Anbieter und Plattformen mit extremen Datenanhäufungen nicht zwingen muss, ihre Algorithmen  
173 ganz oder teilweise offenzulegen, damit Aufsichtsbehörden zumindest eine gewisse Vorstellung  
174 davon bekommen können, welche Daten nach welchen Kriterien zu Profilen verknüpft an Dritte  
175 weiterverkauft werden und ob das bestehende Wettbewerbs- und Kartellrecht nicht angesichts  
176 extremer Datenanhäufungen bei wenigen großen Unternehmen angepasst und fit für das digitale  
177 Zeitalter gemacht werden muss.

178 Bislang ist der Druck auf die Bundesregierung, sich Überwachung und Ausforschung  
179 entgegenzustellen, nicht sonderlich groß. Das wird sich jedoch ändern: Die tatsächlichen  
180 Auswirkungen der derzeit stattfindenden, allumfassenden Vermessung unseres Lebens werden  
181 viele Menschen erst später spüren, dann aber in voller Härte: Aufgrund der falschen Wohnlage  
182 oder Freunde werden sie keine Kredite und keine Versicherungen mehr bekommen. Ihnen wird die  
183 Einreise in Länder verwehrt werden, weil ein Analyseprogramm die Ironie, die in einem  
184 privaten Online-Chat verwendet wurde, nicht erkannt und sie als potentielle Gefährder

185 charakterisiert hat, und sie werden erleben, wie ihr eigenes Auto vor Gericht gegen sie  
186 aussagt.

187 Die Bundesregierung beschäftigt sich mit all diesen Fragen bislang nicht, weil sie weiß,  
188 dass sie selbst höchst ambivalent agiert: Unternehmen verpflichtet man im Rahmen der  
189 anlasslosen Vorratsdatenspeicherung, die sich gegen 80 Millionen Bürger\*innen richtet, neue  
190 Datenberge mit hoch sensiblen Kommunikationsverbindungsdaten anzuhäufen.

191 Während man Deutschland zum „Verschlüsselungsstandort Nummer eins“ auf der Welt machen will,  
192 sinniert man gleichzeitig über das Verbauen von permanenten Hintertüren in Hard- und  
193 Software, die immer auch Kriminellen offenstehen und betätigt sich als Hehler von  
194 Sicherheitslücken auf dem Schwarzmarkt. Hierdurch gefährdet man die IT-Sicherheit und die  
195 Privatheit von Kommunikation massiv. Sämtliche unserer Vorschläge, beispielsweise  
196 durchgehende Ende-zu-Ende-Verschlüsselungen in alle IT-Großprojekte einzuziehen, hat die  
197 Bundesregierung bislang stets abgelehnt. Das rächt sich heute, in Zeiten, in denen  
198 entsprechende Angebote echte Exportschlager wären.

199 Obwohl bis heute der verfassungskonforme Einsatz von in privateste Lebensbereiche  
200 vordringenden „Staatstrojaner“ zur Infiltrierung computertechnischer Systeme nicht  
201 nachgewiesen werden konnte, hält die Bundesregierung an diesem grundrechtlich hoch  
202 umstrittenen Instrument fest und greift noch immer auf das Know-How höchst zweifelhafter  
203 Firmen zurück, die eine Prüfung der Verfassungskonformität durch Einblick in den Quellcode  
204 der Software mit Hinweis auf Betriebs- und Geschäftsgeheimnisse verwehren und ihre mit  
205 deutschem Steuergeld gebaute Technik - durch das Verrücken eines Kommas im Quellcode  
206 aufgetunt - in aller Despotenhände dieser Welt exportieren und dabei helfen, oppositionellen  
207 Protest im Keim zu ersticken und Menschen in Folterkeller zu verbringen.

208 Der sich aus dem Grundgesetz abzuleitenden Verpflichtung, unsere digitale Infrastrukturen  
209 und private Kommunikation effektiv zu schützen, kommt die Bundesregierung bis heute nicht  
210 nach. Bei der EU-Datenschutzreform hat sie eine unrühmliche Rolle gespielt und die so  
211 wichtige Reform, die einen Meilenstein für den Grundrechtsschutz von mehr als 500 Millionen  
212 Europäer\*Innen darstellt, über Jahre ausgebremst und auch hier grundlegende, unseren  
213 Rechtsstaat konstituierende Datenschutzprinzipien wiederholt offen in Frage gestellt.

214 Wichtige Verbündete für uns sind und bleiben die Datenschutzbeauftragten der Länder und des  
215 Bundes sowie die Verbraucherschutzverbände. Sie nehmen auch schon jetzt eine hervorgehobene  
216 und wichtige Rolle im Datenschutz ein. Eine weitere auch institutionelle Stärkung, so dass  
217 jede oder jeder Datenschutzbeauftragte weisungsfrei die eigenen Aufgaben erfüllen kann, ist  
218 unser Ziel. Wie Grüne stellen sicher, dass die Datenschutzbeauftragten ihrer Rolle auch  
219 gerecht werden können. Das ist gerade etwa mit Blick auf die von der EU geschlossenen  
220 Abkommen zum Datenaustausch bisher nicht der Fall. Wir fordern daher, den  
221 Datenschutzaufsichtsbehörden von Bund und Ländern entsprechend den Vorgaben aus dem Urteil  
222 des EuGH vom 6. Oktober 2015 ein normiertes Klagerecht einzuräumen.

### 223 **Transparenz ausbauen und Hass und Hetze bekämpfen**

224 Wir wollen die Chancen der Digitalisierung für die Gesellschaft und die staatlichen Prozesse  
225 noch besser nutzen, unsere Demokratie vitalisieren, das Verhältnis von Bürger\*innen und Staat  
226 reformieren und die Legitimität politischer Entscheidungen erhöhen.

227 Ein besonders positives Beispiel sind die Transparenzgesetze einiger Bundesländer, die die  
228 Verwaltung verpflichten, eine Vielzahl von Dokumenten und Daten kostenfrei und online zur  
229 Verfügung zu stellen. Hier sind insbesondere Hamburg und Rheinland-Pfalz derzeit an der  
230 Spitze. Private Daten werden in dem Verfahren geschützt, in dem das Informationsregister  
231 grundsätzlich keine personenbezogenen Daten enthalten darf. Ein Transparenzgesetz in diesem  
232 Sinne stärkt die demokratische Teilhabe und das Vertrauen in staatliche

233 Entscheidungsprozesse. Wir wollen nicht nur auf Bundesebene ein umfassendes  
234 Transparenzgesetz, sondern auch in den Bundesländern, in denen es solche Gesetze bislang  
235 noch nicht gibt und ermutigen alle, daran aktiv mitzuwirken.

236 Die Pläne des Staates gehen häufig über die bloße Bereitstellung von Informationen hinaus.  
237 Viele Verwaltungsangebote sollen zunehmend online erfolgen. Auch Wirtschaft, Verkehrssysteme  
238 sowie Bildungsnetzwerke sollen weiter digitalisiert werden. Die enormen  
239 Entwicklungspotentiale wollen wir nutzen. Allerdings sind Datenschutz und Datensicherheit  
240 notwendige Voraussetzung für Vertrauen in diese neuen digitalen Angebote. Nur dann werden  
241 die Bürger\*Innen die Vorteile der Digitalisierung langfristig annehmen und entsprechende  
242 Angebote unbeschwert nutzen. Das bedeutet, Verfahren und Geschäftsprozesse müssen von Beginn  
243 an so konzipiert, strategisch angeleitet, umgesetzt und praktiziert werden, dass sie der  
244 informationellen Selbstbestimmung und der Vertraulichkeit und Integrität  
245 informationstechnischer Systeme Rechnung tragen. Prinzipien des Datenschutzes, der  
246 Informationsfreiheit und -sicherheit wie etwa der Gesetzesvorbehalt, die Erforderlichkeit,  
247 die Datenerhebung beim Betroffenen, Privacy by Design und Default, die Zweckbindung der  
248 Daten, Datenvermeidung und -sparsamkeit, Schutzbedarfsfeststellung und Risikoanalyse sowie  
249 Datensicherheit durch technische und organisatorische Maßnahmen sind zwingend zu  
250 berücksichtigen. Die zunehmende Verdattung unseres Alltagslebens führt dazu, dass  
251 umfassendste Datenprofile über uns alle entstehen, die Datensouveränität ist daher zu  
252 stärken und der Trend der allumfassenden Verdattung und Algorithmisierung muss mit Konzepten  
253 der Risikorelevanz und entsprechenden Schutz- und Nicht-Verarbeitungsvorgeben dieser Daten  
254 einhergehen.

255 Anders als es auf den ersten Blick erscheint, erweitert das Internet nicht nur meine  
256 Möglichkeiten, mich selbstbestimmt zu entwickeln. Teilweise ist das Gegenteil der Fall.  
257 Immer mehr Unternehmen nehmen für sich in Anspruch, vor mir zu wissen, was ich demnächst  
258 kaufen werde, wo ich meinen Urlaub verbringen möchte oder in wen ich mich verlieben könnte.  
259 Algorithmen filtern die unzähligen Angebote für mich heraus. Das ist vielleicht bequem, aber  
260 nicht unbedingt gut für unsere Gesellschaft. Wir müssen Gefahren durch eine intransparente  
261 Beeinflussung des Willensbildungsprozesses durch Hyper Targeting und Big Nudging erkennen,  
262 um darauf auch angemessen reagieren zu können. Dies gilt insbesondere für Werbung im Rahmen  
263 von Wahlkämpfen. Wir Grüne lehnen es ab, einzelne Wählerinnen und Wähler durch die  
264 Ausnutzung von Datenprofilen so genau zu beeinflussen, um auf einen Kern unserer Demokratie,  
265 die freie Wahl, massiven Einfluss zu nehmen. Politisches Targeting gehört reguliert und wir  
266 rufen die anderen Parteien dazu auf, unserer Nichtnutzung zu folgen.

267 Doch nicht nur die Nutzung und Ausnutzung von Daten über uns beeinflussen unser Handeln,  
268 unsere Kommunikation und soziales Zusammenleben. Wir erleben, wie im digitalen Diskurs eine  
269 Verrohung stattfinden, engagierte Menschen, ganz egal ob Feminist\*innen, Politiker\*innen,  
270 Ehrenamtliche, Journalist\*innen oder Menschen mit Migrationshintergrund werden immer  
271 häufiger angefeindet, beleidigt und bedroht. Die Hoffnung, dass durch das Internet eine neue  
272 Debattenkultur und die Möglichkeiten des freien Wissenszugangs zu mehr Toleranz und  
273 Solidarität führen, wurde leider nicht erfüllt. Stattdessen entstehen derzeit abgeschottete  
274 Räume der selbstreferentiellen Meinungs austausches. Hate Speech und Hasspropaganda stellen  
275 eine Bedrohung für unsere offene Gesellschaft dar. Einschüchterungen und Straftaten, müssen  
276 mit allen rechtsstaatlichen Mitteln verfolgt werden. Der Ausweitung der privaten  
277 Rechtsdurchsetzung widersprechen wir, stattdessen braucht es einen Ausbau der Kapazitäten  
278 bei Polizei und Staatsanwaltschaften in diesem Bereich, einfachere Wege solche Inhalte zu  
279 melden und anzuzeigen und eine Bundesregierung die es nicht länger verpasst,  
280 milliardenschwere Unternehmen an ihre gesellschaftliche und rechtliche Verpflichtung zu  
281 erinnern, entsprechende Inhalte konsequent zu überprüfen, zu löschen und an die  
282 Strafverfolgungsbehörden weiterzuleiten.

283 Aktuell beobachten wir, dass die Zahl rechtsextremer Straftaten zunimmt – erschütternde  
284 Beispiele sind Brandanschläge auf Flüchtlingsunterkünfte und gewaltsame Übergriffe mit  
285 fremdenfeindlichem Hintergrund. Und die Radikalisierung im Internet spielt dabei eine  
286 gewichtige Rolle. Mit allen rechtsstaatlichen Mitteln muss der Staat rechten Terror,  
287 alltäglichen Rassismus und institutionell verankerten Rassismus bekämpfen. Dazu zählt  
288 selbstverständlich auch das Strafrecht. Strafbarkeitslücken bei dem Verbreiten und Verwenden  
289 von Propagandamitteln und Kennzeichen verfassungswidriger Organisationen bei Handlungen im  
290 Ausland sind zu schließen und unter Strafe zu stellen. Zudem ist eine stärkere  
291 Berücksichtigung menschenverachtender Beweggründe bei der Strafzumessung gesetzlich zu  
292 verankern.

293 Dieser Antrag ist in Zusammenarbeit von Till Steffen, Konstantin von Notz, Jan Philipp  
294 Albrecht und Malte Spitz entstanden.

## **Begründung**

erfolgt mündlich

## **Unterstützer\*innen**

Eka von Kalben (Schleswig-Holstein); Yvonne Paul (BAGen); Irene Mihalic (NRW)