

Antrag 180/I/2024**Jusos LDK****Der Landesparteitag möge beschließen:****Der Bundesparteitag möge beschließen:****Empfehlung der Antragskommission****Überweisen an: ASJ, FA III - Innen- und Rechtspolitik, Forum Netzpolitik (Konsens)****Hände weg von meinen Chats! - Gegen Chatkontrolle und Überwachung im Internet**

1 Der Kongress der Party of European Socialists möge be-
2 schließen:

3

4 „**Privacy is the right to a free mind**“ - Was bisher geschah
5 Vor 10 Jahren, im Sommer 2013, versetzte der NSA-
6 Mitarbeiter Edward Snowden die Welt in Aufruhr: Mit der
7 Veröffentlichung geheimer Daten und Materialien konn-
8 te er beweisen, dass die Geheimdienste der USA ihre eige-
9 nen und auch fremde Staatsbürger*innen gezielt – auch
10 das Handy der damaligen Bundeskanzlerin Angela Mer-
11 kel wurde überwacht – aber auch großflächig und unge-
12 richtet abhörten. Diese permanente Überwachung und
13 Aufzeichnung von Bewegungsdaten, Kommunikation und
14 Bildern erlaubte es den Geheimdiensten, auch Jahre nach
15 der Aufzeichnung detaillierte Profile über Personen zu er-
16 stellen. Diese Form der unbegründeten und rechtswidri-
17 gen massenhaften Überwachung und Vorratsdatenspei-
18 cherung stieß damals zu Recht auf weltweite massive Em-
19 pörung.

20

21 Seit den Leaks von Edward Snowden hat sich an der Praxis
22 der Geheimdienste wahrscheinlich wenig geändert. Die
23 Möglichkeiten, die eigene Kommunikation zu verschlüs-
24 seln und so vor dem Zugriff Dritter zu schützen, wurden
25 aber ausgeweitet. Was vor 10 Jahren noch ein Hobby von
26 wenigen Personen war, ist spätestens mit der Einführung
27 von Ende-zu-Ende-Verschlüsselung bei Messengerdiens-
28 ten in der Breite der Gesellschaft angekommen. Ende-
29 zu-Ende-Verschlüsselung erlaubt es Nutzer*innen, priva-
30 te Kommunikation zu führen, ohne dass die Nachrichten
31 von Messengerdiensten, Regierungen oder anderen unbe-
32 fugten Personen gelesen werden kann – ein riesiger Fort-
33 schritt für Privatsphäre und sichere Kommunikation im In-
34 ternet.

35

36 Im Mai 2022 stellte die schwedische EU-Kommissarin Yl-
37 va Johansson einen Gesetzesvorschlag vor, der das Ende
38 für verschlüsselte Kommunikation und Anonymität im In-
39 ternet bedeuten könnte. „Child Sexual Abuse Reduction“
40 nennt sich dieses Vorhaben und das Ziel ist es, Kindes-
41 missbrauch und die Verbreitung von diesen im Netz einzu-
42 dämmen. Wir unterstützen das grundlegende, obligatori-
43 sche Anliegen, der Unterbindung von Darstellungen sexu-
44 ellen Kindesmissbrauchs, jedoch nicht diesen Weg dort-
45 hin. Denn dazu sollen neben der massenhaften Kontrolle
46 von Chats auch Altersverifikation und Netzsperrern einge-
47 setzt werden.

48

**49 Meine Chats gehören mir – und nicht einer KI oder den
50 Behörden!**

51 Ylva Johansson schlägt in ihrem Gesetzentwurf verschie-
52 dene Maßnahmen vor, die technische Umsetzung bleibt
53 dabei unklar.

54

55 Zentral in der Debatte um diesen Entwurf ist die soge-
56 nannte Chatkontrolle: die Kommission hat das Ziel formu-
57 liert, alle Chats auf Kindesmissbrauch zu scannen.

58

59 Die Einführung einer Chatkontrolle würde dazu führen,
60 dass die private Kommunikation jeder Person zu jeder Zeit
61 gescannt würde. Dies würde einen massiven Einschnitt in
62 die Bürger*innenrechte bedeuten.

63

64 Dass man verschlüsselte Kommunikation nicht einfach
65 verbieten kann, ist zum Glück selbst Ylva Johansson klar.
66 Die Alternative heißt „client-side scanning“: jede Nach-
67 richt würde, bevor sie verschickt wird, auf dem eige-
68 nen Gerät gescannt und mit einer zentralen Datenbank
69 aus Darstellungen sexuellen Kindesmissbrauchs vergli-
70 chen. In der Logik der EU-Kommission wird dadurch die
71 Verschlüsselung der Kommunikation nicht angegriffen,
72 schließlich wird die Nachricht erst gescannt und erst da-
73 nach verschlüsselt.

74

75 Doch das Gegenteil ist der Fall. Die Einführung dieser Tech-
76 nologie einen massiven Einschnitt in die Privatsphäre dar-
77 stellen und nach Einschätzung des legal councils der EU
78 die Essenz der fundamentalen Rechte verletzen. Auch die
79 Expert*innen, die der Digitalausschuss des Bundestages
80 im März zu einer Anhörung eingeladen hat, haben sich
81 einmündig gegen client-side-scanning ausgesprochen.
82 Von Kinderschutzbund und Internet-Ermittler bis Chaos
83 Computer Club – nicht einmal der Union ist es gelungen,
84 eine*n Expert*in aufzutreiben, der*die sich für die vor-
85 geschlagenen Maßnahmen ausspricht. Auch der wissen-
86 schaftliche Dienst des Bundestags sieht im aktuellen Ver-
87 ordnungsentwurf „unverhältnismäßige Eingriffe in die ge-
88 prüften Grundrechte der GRCh (EU-Grundrechtecharta).

89

90 Auch technisch zeigen sich Problematiken: damit eine KI
91 Missbrauchsabbildungen erkennen kann, muss sie vor-
92 her auf einer Sammlung von solchen Abbildungen trai-
93 niert werden. Dabei werden der KI Abbildungen gezeigt
94 und die KI soll die Abbildungen als Missbrauch oder nicht
95 deklarieren. Die Entscheidungen der KI im Trainingspro-
96 zess müssen von Menschen kontrolliert werden, die sich
97 ebenfalls diese Abbildungen ansehen und die Entschei-
98 dung der KI bestätigen müssen. Eine solche unbekannte
99 KI bietet massives Missbrauchspotential. Verbrecher*in-
100 nen könnten Zugriff auf Trainingsdaten erlangen und die-

101 se Abbildungen weiter nutzen oder sich durch die KI selbst
102 Bilder generieren lassen. Weiterhin kann von Bürger*in-
103 nen nicht kontrolliert werden, ob die eigenen Nachricht-
104 ten tatsächlich nur in diesem Rahmen kontrolliert oder ob
105 auch andere Inhalte gesucht werden.

106

107 Jede*r Bürger*in wäre davon betroffen, dass sämtliche pri-
108 vate Kommunikation ständig durchsucht würde. Von ei-
109 ner zentralen unbekanntem Entität. Neben echten Miss-
110 brauchsabbildungen würde diese Kontrolle auch jede
111 Menge falsche Meldungen produzieren, also Nachrichten,
112 die fälschlich als Missbrauch gekennzeichnet werden und
113 dann von den Behörden kontrolliert werden. Dies kann so-
114 wohl das Versenden von Kinderfotos in Familiengruppen
115 als auch Nachrichten betreffen, die sich Jugendliche ein-
116 vernehmlich schicken. Studien zeigen zudem, dass Inhal-
117 te, die die queere Community betreffen, deutlich häufiger
118 fälschlich als Pornographie erkannt werden.

119

120 Zudem ist fragwürdig, ob die Einführung der Chatkontrol-
121 le tatsächlich einen Beitrag zu weniger Kindesmissbrauch
122 leisten würde. Missbrauchsabbildungen werden in der Re-
123 gel nicht per Messenger versendet. Stattdessen werden
124 Links auf Seiten im „dark net“ geteilt, von denen das Ma-
125 terial anonym abgerufen werden kann.

126

127 Die Einführung einer Chatkontrolle würde das zugrunde-
128 liegende Problem also nicht lösen, sondern unverhältnis-
129 mäßig in die Privatsphäre aller eingreifen.

130

131 **Keine Stoppschilder im Internet – Löschen, statt sperren!**

132 Schon 2009 sagte Ursula von der Leyen, damals noch als
133 Familienministerin, Abbildungen von sexualisierter Ge-
134 walt gegen Kinder im Internet den Kampf an. Ihr Vor-
135 schlag: Seiten, auf denen Darstellungen sexuellen Kin-
136 desmissbrauchs zu finden sind, sollen gesperrt und mit
137 einem großen Stoppschild versehen werden. Dieser Vor-
138 schlag wurde damals nach langen Protesten aufgegeben.
139 Zu Recht! Netzsperrungen sind nicht nur schwer umzusetzen
140 und lassen sich leicht umgehen. Wird eine Seite mit einem
141 großen roten Stoppschild versehen, wird auch noch akti-
142 ver Täter*innenschutz betrieben. Alle Materialien existie-
143 ren noch auf den Servern der gesperrten Seite und können
144 von Betreiber*innen einfach auf eine andere Seite über-
145 tragen werden.

146

147 Stattdessen wird in Deutschland inzwischen das Prin-
148 zip „Löschen, statt Sperren“ verfolgt. Stoßen Ermittler*in-
149 nen im Internet auf Darstellungen sexuellen Kindesmiss-
150 brauchs, wird dies an die Serverbetreiber*innen gemeldet,
151 die die Seite mit allen Inhalten löschen. Dieses Verfahren
152 ist „einfach und wirksam“, so berichtet es das Justizmi-
153 nisterium. Und doch werden viele Seiten nicht direkt ge-

154 löscht. Den Behörden fehlt häufig Personal, um alle Sei-
155 ten zu löschen. Es ist nicht hinnehmbar, dass einfache Mit-
156 tel, die ausschließlich Täter*innen betreffen, durch Ermitt-
157 lungsbehörden nicht ausgeschöpft werden.

158

159 Netzsperrern sind auch auf europäischer Ebene zu verhin-
160 dern. Stattdessen müssen Missbrauchsabbildungen wo
161 immer sie auftreten, gelöscht werden. Behörden müssen
162 ausreichend Personal ausgestattet sein, um Seiten zu lö-
163 schen.

164

165 **Alter, geht's noch? - Ein Internet ohne Altersverifikation** 166 **und Ausweispflicht**

167 Die Kommission geht in ihrem Gesetzesvorhaben aber
168 noch weiter, als bestehendes Material zu erkennen. Auch
169 dem sogenannten „grooming“ - also versuchter Kontakt-
170 aufnahme von Erwachsenen bei Kindern mit dem Ziel des
171 Missbrauchs soll Einhalt geboten werden. Dafür könnten
172 Anbieter*innen künftig dazu gezwungen werden, Alters-
173 kontrollen einzuführen.

174

175 Heute schon verhindern manche Anbieter*innen, dass
176 Kinder von Erwachsenen angeschrieben werden kön-
177 nen. TikTok beispielsweise stellt Accounts von 13- bis 15-
178 jährigen grundsätzlich privat. Solche Maßnahmen basie-
179 ren meist auf Selbstauskünften der Nutzer*innen, dies
180 wird der EU-Kommission sicher nicht ausreichen.

181

182 Möglichkeiten der Altersverifikation reichen von der Iden-
183 tifikation mit Ausweisen bis zur KI-gestützten Berech-
184 nung des Alters durch biometrische Daten. Nicht nur aus
185 Datenschutzperspektive ist dabei eine Variante schlim-
186 mer als die nächste.

187

188 Die Verifikation des Alters durch Kontrolle des Personal-
189 ausweises würde das Ende der Anonymität im Internet be-
190 deuten. Nutzer*innen jeder Plattform, auf der Chats mög-
191 lich sind, müssten den Anbieter*innen persönliche Da-
192 ten übermitteln. Ein Datenleak oder ein Hackerangriff auf
193 die Datenbanken der Anbieter*innen wäre fatal. Durch
194 die AusweisApp ist es theoretisch möglich, nur die Daten
195 zu übermitteln, die tatsächlich gebraucht werden. Es ist
196 jedoch abzusehen, dass sich Plattformen mit dieser Ein-
197 schränkung nicht zufriedengeben werden, sondern unter
198 den Deckmantel gesetzlicher Legitimierung weitere Da-
199 ten zu Werbezwecken sammeln werden und so weitere
200 Daten von Nutzer*innen sammeln können, die sie eigent-
201 lich nicht haben sollten.

202

203 Der Angriff auf die Anonymität im Internet hat aber auch
204 weitere Auswirkungen, die zu kritisieren sind. Die Pflicht,
205 für jede Form der Online-Kommunikation den Personal-
206 ausweis vorlegen zu müssen, wird massive Auswirkungen

207 auf die Kommunikationsfreiheit im Internet haben. Wenn
208 Nutzer*innen bei jeder Anmeldung und Nachricht im In-
209 ternet befürchten müssen, dass Inhalte gelesen und zu-
210 rückverfolgt werden können, hat dies messbare Folgen für
211 das individuelle Verhalten und die Meinungsfreiheit. Es ist
212 zudem unverhältnismäßig: Niemand würde auf die Idee
213 kommen, vor jedem Gespräch, Telefonat oder Museums-
214 besuch einen Personalausweis anzufordern.

215

216 Personen, die keinen Ausweis besitzen, wären so komplett
217 von digitaler Teilhabe ausgeschlossen. Auch Betreiber*in-
218 nen von Open-Source-Programmen wären von einer sol-
219 chen Regelung bedroht. Open-Source-Programme ermög-
220 lichen es Nutzer*innen, Programme kostenlos zu nutzen,
221 weiterzuentwickeln und zu testen. Dabei gibt es keine
222 zentrale Datenbank von Nutzer*innen, sondern Program-
223 me oder Quellcode können aus verschiedenen Quellen ge-
224 nutzt werden. Der Schutz der persönlichen Daten von Nut-
225 zer*innen muss auch im Internet gelten!