

Antrag 150/I/2022**KDV Neukölln****Der Landesparteitag möge beschließen:****Hände weg von den Daten - Kein Big Data für die Polizei!**

1 Durch die fortschreitende Digitalisierung lassen sich immer
2 mehr Daten über Menschen und ihr Leben erheben.
3 Diese Daten entstehen maßgeblich im digitalen Raum.
4 So zeigen immer wieder Untersuchungen, dass Unmen-
5 gen an Daten im Internet über die Nutzer*innen gesamt-
6 melt werden – oftmals ohne ihr Wissen. Weiterhin gibt
7 es Berichte, dass selbst digitale Profile von Menschen von
8 Diensten angelegt werden, die diese Dienste (z.B. Face-
9 book) gar nicht selbst nutzen. Klar ist: Es werden immer
10 mehr Daten über Menschen erhoben, ob sie es wissen
11 oder nicht.

12
13 Im Zuge der Pandemiebekämpfung wurden auch Apps
14 zur Kontaktnachverfolgung eingesetzt. So arbeitete die
15 Corona-Warn-App mit Open Source (also einem öffent-
16 lich einsehbar und bearbeitbaren Code) und möglichst
17 datensparsam, um die notwendigen Daten zur Kontaktnach-
18 nachverfolgung zu erheben. Neben der von der öffent-
19 lichen Hand finanzierten Corona-Warn-App gab es auch
20 kommerzielle Alternativen, wie die Luca-App. Diese wurde
21 vor allem zur Kontaktnachverfolgung in Restaurants
22 eingesetzt. Dazu musste allerdings immer ein Name ein-
23 gegeben werden, sodass die Nutzung - anders als bei
24 der Corona-Warn-App - nicht anonym war. Diese fehlen-
25 de Anonymität versuchte sich die Polizei in mehreren Län-
26 dern zunutze zu machen. So wurde beispielweise in Mainz
27 ohne Rechtsgrundlage seitens der Polizei auf Daten aus
28 der Luca-App zurückgegriffen, um Zeug*innen in einem
29 mutmaßlichen Tötungsdelikt ausfindig zu machen. Das
30 heißt, in diesem Fall wurden ohne richterlichen Beschluss,
31 die persönlichen Daten von Unbeteiligten abgefragt. In
32 Baden-Württemberg gab es ähnliche Fälle und auch in
33 Brandenburg kündigte die Polizei an, dass Daten aus der
34 Luca-App genutzt werden sollten.

35
36 Dies sind allerdings nicht die einzigen Fälle, in denen
37 Strafverfolgungsbehörden Daten von Unbeteiligten mas-
38 senhaft abgreifen. So beschloss vor kurzem das bayeri-
39 sche Landeskriminalamt, die umstrittene Software Palan-
40 tir einzusetzen. Diese Software wird bereits von Hessen
41 genutzt und setzt das sogenannte Datenmining ein. Da-
42 bei werden Daten aus verschiedenen Datenbanken mit-
43 einander verknüpft. Palantir ist für den Bereich der Big Da-
44 ta, also sehr große Datenmengen, konzeptioniert. Zwar
45 soll die Software nach Angaben des bayerischen LKAs
46 nicht mit dem Internet verbunden werden und keine neu-
47 en Daten erhoben werden, aber dennoch werden Daten
48 nicht für den Zweck verwendet, für den sie ursprünglich

Empfehlung der Antragskommission**Überweisen an: ASJ, FA III - Innen- und Rechtspolitik, Fo-
rum Netzpolitik (Konsens)**

49 gespeichert worden sind. Die Wahrscheinlichkeit, dass
50 Daten so zweckentfremdet werden, ist dadurch sehr groß.
51 Die Software soll für Terrorismusbekämpfung eingesetzt
52 werden. Allerdings werden durch die Verknüpfung von
53 Datenbanken auch massiv persönliche Daten von Men-
54 schen abgefragt, die nicht im Kontext von Terrorismus-
55 bekämpfung erhoben worden sind. Der bayerische Lan-
56 desdatenschutzbeauftragte hält dies für einen deutlichen
57 Eingriff in die Grundrechte vieler Menschen. Wie genau
58 welche Daten abgefragt und verknüpft werden, ist zudem
59 nicht öffentlich bekannt. Der Vertrag, den die bayerische
60 Polizei mit Palantir abgeschlossen hat, ist so ausgelegt,
61 dass andere Länder und auch der Bund diesem leicht bei-
62 treten und die Software auch nutzen können. Viele Ex-
63 pert*innen hegen allerdings Zweifel an der Datenschutz-
64 und Verfassungskonformität der Software. Nach Berich-
65 ten hat das Unternehmen seine Produkte auch der Berli-
66 ner Polizei vorgestellt. Für uns ist ein Einsatz einer Soft-
67 ware, die nachweislich im Widerspruch zum Grundgesetz
68 steht, nicht hinnehmbar. Wir lehnen eine solche Koopera-
69 tion strikt ab.

70

71 Die Daten, die von Strafverfolgungsbehörden in Deutsch-
72 land erhoben werden, sind hochsensibel. Immer wieder
73 gab es in den letzten Jahren Berichte darüber, dass Adres-
74 sen von Aktivist*innen, Politiker*innen oder Prominenten
75 ohne Rechtsgrundlage abgefragt worden sind. Fast wö-
76 chentlich gibt es neue Berichte über rechtsextreme Po-
77 lizist*innen. Der Einsatz undurchsichtiger, umstrittener
78 und datenschutzrechtlich hoch zweifelhafter Software
79 wird diese angespannte Lage nicht verbessern. Stattdes-
80 sen müssen Menschen nun Sorge haben, dass ihre Daten
81 ohne Grund auf einmal in Terrorismuskontexten auftau-
82 chen, nur weil eine Software dies entschieden hat. Die
83 neuen Möglichkeiten, die sich auch für Strafverfolgungs-
84 behörden durch die Digitalisierung ergeben, dürfen kein
85 Freifahrtschein für Grundrechtseinschränkungen sein.

86

87 Wir fordern daher:

- 88 • Die Berliner Polizei wird weder die Luca-App, noch
89 vergleichbare Apps ohne richterlichen Beschluss für
90 die Strafverfolgung oder andere Ermittlungen nut-
91 zen.
- 92 • Die Berliner Polizei wird Auswertung- und Analyse-
93 software wie z.B. Palantir nicht für die Auswertung
94 eingriffsintensitätsarmer Daten nutzen.
- 95 • Berlin wird sich auf Bundesebene dafür einsetzen,
96 dass strenge Datenschutzmaßgaben insbesondere
97 an den polizeilichen Umgang mit Daten beschlos-
98 sen und umgesetzt werden. Das Ziel dieser Maßga-
99 ben muss sein, Grundrechte zu schützen und den
100 Einsatz sowie den Kauf von Software wie Palantir zu
101 unterbinden.

102

|