

A7 Alle Cookiedaten-Ankäufe Blockieren - keine Nutzung kommerzieller Daten durch die Polizei!

Gremium: Landesvorstand
Beschlussdatum: 19.08.2026

Antragstext

1 Unser Smartphone ist längst zum ständigen Begleiter geworden. Es navigiert uns
2 durch den Alltag, zeigt das Wetter an, hilft beim Sport oder beim Einkaufen.
3 Gleichzeitig erzeugen unzählige Apps fortlaufend Standortdaten. Viele dieser
4 Daten werden nicht benötigt, um die jeweilige App bereitzustellen, sondern
5 dienen Werbezwecken. Sie werden gesammelt, analysiert und über ein kaum
6 reguliertes Netzwerk von Datenhändler:innen weiterverkauft. Aus scheinbar
7 harmlosen Einzelinformationen entstehen detaillierte Bewegungsprofile, die
8 erkennen lassen, wo Menschen wohnen, arbeiten, ihre Freizeit verbringen oder
9 welche Ärzt:innen, religiösen Einrichtungen, Beratungsstellen oder politischen
10 Veranstaltungen sie aufsuchen.

11 Diese Daten betreffen dabei regelmäßig nicht einzelne Verdächtige, sondern
12 Millionen unbeteiligter Menschen. Gerade deshalb unterliegen staatliche Zugriffe
13 auf vergleichbare Informationen im deutschen Recht hohen rechtsstaatlichen
14 Anforderungen. So bedürfen etwa Funkzellenabfragen oder andere Maßnahmen zur
15 Erhebung von Telekommunikations- und Standortdaten grundsätzlich spezieller
16 gesetzlicher Grundlagen und teilweise richterlicher Anordnungen.

17 Durch den wachsenden Markt kommerzieller Datenhändler:innen droht jedoch ein
18 gefährlicher Umgehungsweg zu entstehen. Wenn Behörden dieselben oder
19 vergleichbare Informationen nicht bei Telekommunikationsunternehmen, sondern von
20 privaten Datenhändler:innen erwerben, besteht die Gefahr, dass rechtsstaatliche
21 Schutzmechanismen faktisch unterlaufen werden. Was der Staat selbst nur unter
22 engen Voraussetzungen erheben dürfte, könnte so auf einem kommerziellen Markt
23 eingekauft werden.

24 Der Umgang deutscher Sicherheitsbehörden mit kommerziell gehandelten
25 Standortdaten ist geprägt von Intransparenz und uneinheitlicher Praxis. Während
26 fünf Landeskriminalämter angaben, keine kommerziellen Standortdaten zu nutzen,
27 verweigerten zahlreiche Behörden eine Auskunft. Die Landeskriminalämter
28 Brandenburg und Mecklenburg-Vorpommern bestätigten, Dienstleistungen von
29 Datenhändler:innen in Anspruch zu nehmen bzw. genommen zu haben. Das Thüringer
30 Landeskriminalamt erklärte, der Einsatz kommerziell erhältlicher Standortdaten
31 sei rechtlich grundsätzlich möglich, verweigerte jedoch aus „polizeitaktischen
32 Gründen“ die Auskunft darüber, ob entsprechende Daten tatsächlich genutzt
33 werden. Auch Bundespolizei und Bundeskriminalamt beantworteten entsprechende
34 parlamentarische Nachfragen nicht.

35 Gerade diese Intransparenz ist höchst problematisch. In einem Rechtsstaat muss
36 nachvollziehbar sein, auf welcher gesetzlichen Grundlage tiefgreifende
37 Grundrechtseingriffe erfolgen. Die informationelle Selbstbestimmung gehört zu
38 den im Grundgesetz festgeschriebenen Grundrechten. Bürger:innen müssen darauf

39 vertrauen können, dass personenbezogene Daten nur zu dem Zweck verwendet werden,
40 zu dem sie erhoben wurden. Werden Standortdaten ursprünglich zu Werbezwecken
41 verarbeitet und später für Strafverfolgung oder Gefahrenabwehr genutzt, liegt
42 regelmäßig eine Zweckänderung vor, die besonders hohen rechtlichen Anforderungen
43 unterliegt.

44 Hinzu kommt, dass bereits die Herkunft vieler Datensätze erhebliche
45 datenschutzrechtliche Fragen aufwirft. Nach der Datenschutz-Grundverordnung und
46 der ePrivacy-Richtlinie setzt die Verarbeitung und Weitergabe personenbezogener
47 Standortdaten grundsätzlich eine informierte und freiwillige Einwilligung der
48 Betroffenen voraus. Dennoch existiert europaweit ein milliardenstarker Markt,
49 auf dem detaillierte Bewegungsprofile gehandelt werden. Es bestehen erhebliche
50 Zweifel, ob zahlreiche Geschäftsmodelle der Datenbroker den Anforderungen des
51 europäischen Datenschutzrechts tatsächlich genügen. Dennoch existiert europaweit
52 ein milliardenstarker Markt, auf dem Bewegungsprofile gehandelt werden.
53 Internationale Recherchen zeigen, dass zu den Kund:innen solcher
54 Datenhändler:innen unter anderem Polizeibehörden in Ungarn sowie die US-
55 Einwanderungsbehörde ICE gehören. Damit entsteht nicht nur ein erhebliches
56 Risiko für die Privatsphäre der Betroffenen, sondern auch für die innere und
57 äußere Sicherheit: Umfangreiche Bewegungsprofile können für Spionage,
58 Desinformation oder andere nachrichtendienstliche Zwecke missbraucht werden.

59 Auch die rechtliche Grundlage für den Ankauf solcher Daten ist zweifelhaft. Der
60 Wissenschaftliche Dienst des Deutschen Bundestages kommt zu dem Ergebnis, dass
61 allgemeine Ermittlungsbefugnisse beziehungsweise Ermittlungs-Generalklauseln
62 angesichts der Eingriffsintensität umfangreicher kommerzieller Bewegungsprofile
63 voraussichtlich keine ausreichende Rechtsgrundlage darstellen. Vielmehr spreche
64 vieles dafür, dass hierfür spezielle gesetzliche Ermächtigungen erforderlich
65 wären.

66 Gerade deshalb darf sich der Staat nicht zum Kunden eines Geschäftsmodells
67 machen, das auf der massenhaften Sammlung und Vermarktung personenbezogener
68 Bewegungsdaten beruht. Wer Daten ankauft, schafft Nachfrage und stärkt einen
69 Markt, dessen wirtschaftlicher Erfolg davon abhängt, möglichst umfassend
70 Informationen über das Leben von Millionen Menschen zu sammeln und zu verwerten.
71 Damit wird ausgerechnet ein Geschäftsmodell finanziert, das erhebliche
72 datenschutz- und verfassungsrechtliche Fragen aufwirft.

73 Das widerspricht dem Selbstverständnis eines demokratischen Rechtsstaats.
74 Aufgabe des Staates ist es, Grundrechte zu schützen und die wirtschaftliche
75 Macht dort zu begrenzen, wo sie Freiheitsrechte gefährdet. Ermittlungsbefugnisse
76 müssen sich aus demokratisch legitimierten Gesetzen ergeben, nicht aus der
77 Verfügbarkeit käuflicher Datenbestände oder der technischen Möglichkeit, diese
78 zu erheben.

79 Gerade in einer zunehmend datengetriebenen Wirtschaft muss deshalb gelten: Der
80 Staat reguliert den Markt, nicht der Markt den Staat. Öffentliche Sicherheit
81 darf nicht davon abhängen, wie umfassend private Unternehmen das Leben von
82 Millionen Menschen überwachen und zu Geld machen können. Nicht der Staat darf
83 Kunde des Datenmarktes werden, der Datenmarkt muss Gegenstand staatlicher
84 Regulierung sein.

85 Wir fordern daher:

86 1. **Bundesweites Verbot des Ankaufs und der Nutzung kommerziell gehandelter**
87 **Standort- und Bewegungsdaten durch Polizei- und Sicherheitsbehörden.**

88 Der Erwerb und die Nutzung personenbezogener Standort- und Bewegungsdaten
89 aus dem kommerziellen Datenhandel dürfen nicht Teil staatlicher
90 Ermittlungs- oder Gefahrenabwehrmaßnahmen sein. Der Staat darf keinen
91 Markt finanzieren oder legitimieren, dessen Geschäftsmodell auf der
92 massenhaften Verwertung personenbezogener Daten beruht.

93 2. **Umfassende datenschutzrechtliche Überprüfung der bisherigen Praxis durch**
94 **die Datenschutzaufsichtsbehörden.**

95 Die zuständigen Landesdatenschutzbeauftragten sowie der Bundesbeauftragte
96 für den Datenschutz und die Informationsfreiheit sollen prüfen, ob der
97 Ankauf und die Nutzung kommerzieller Standortdaten durch
98 Sicherheitsbehörden mit den Vorgaben der DSGVO sowie dem Grundrecht auf
99 informationelle Selbstbestimmung vereinbar sind. Festgestellte Verstöße
100 müssen konsequent beanstandet und beendet werden.

101 3. **Verbindliche Transparenz- und Berichtspflichten für Sicherheitsbehörden**
102 **gegenüber den Parlamenten.**

103 Parlamente müssen nachvollziehen können, ob und in welchem Umfang
104 Sicherheitsbehörden kommerzielle personenbezogene Datensätze erwerben oder
105 nutzen. Art, Umfang, Rechtsgrundlage und Zweck solcher Datenkäufe sind
106 regelmäßig offenzulegen.

107 4. **Konsequente Regulierung des Handels mit personenbezogenen Standort- und**
108 **Bewegungsdaten.**

109 Unternehmen, die personenbezogene Standortdaten sammeln, aufbereiten oder
110 weiterverkaufen, müssen einer wirksamen datenschutzrechtlichen Kontrolle
111 unterliegen. Geschäftsmodelle, die auf der massenhaften Vermarktung
112 personenbezogener Bewegungsprofile beruhen, dürfen keinen Platz im
113 europäischen Binnenmarkt haben.

114 5. **Keine Aufnahme einer Befugnis zum Ankauf oder zur Nutzung kommerziell**
115 **gehandelter Standortdaten in das neue Thüringer Polizeiaufgabengesetz.**

116 Im Zuge der aktuellen Novellierung des Thüringer Polizeiaufgabengesetzes
117 dürfen keine Rechtsgrundlagen geschaffen werden, die den Ankauf oder die
118 Nutzung kommerzieller Standort- und Bewegungsdaten ermöglichen oder
119 erleichtern. Thüringen darf die bestehenden rechtlichen Unsicherheiten
120 nicht durch neue Überwachungsbefugnisse verschärfen.

Begründung

Erfolgt mündlich.