R03 Alle Cookiedaten-Ankäufe Blockieren - keine Nutzung kommerzieller Daten durch die Polizei!

Gremium:	Landesvorstand
Beschlussdatum:	19.08.2026
Tagesordnungspunkt:	6 Antragsberatung

Antragstext

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

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

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

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

Gerade diese Intransparenz ist höchst problematisch. In einem Rechtsstaat muss nachvollziehbar sein, auf welcher gesetzlichen Grundlage tiefgreifende Grundrechtseingriffe erfolgen. Die informationelle Selbstbestimmung gehört zu

den im Grundgesetz festgeschriebenen Grundrechten. Bürger:innen müssen darauf vertrauen können, dass personenbezogene Daten nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden. Werden Standortdaten ursprünglich zu Werbezwecken verarbeitet und später für Strafverfolgung oder Gefahrenabwehr genutzt, liegt regelmäßig eine Zweckänderung vor, die besonders hohen rechtlichen Anforderungen unterliegt.

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

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

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

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

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

Wir fordern daher:

1. **Bundesweites Verbot des Ankaufs und der Nutzung kommerziell gehandelter Standort- und Bewegungsdaten durch Polizei- und Sicherheitsbehörden.**
   Der Erwerb und die Nutzung personenbezogener Standort- und Bewegungsdaten aus dem kommerziellen Datenhandel dürfen nicht Teil staatlicher Ermittlungs- oder Gefahrenabwehrmaßnahmen sein. Der Staat darf keinen Markt finanzieren oder legitimieren, dessen Geschäftsmodell auf der massenhaften Verwertung personenbezogener Daten beruht.

2. **Umfassende datenschutzrechtliche Überprüfung der bisherigen Praxis durch die Datenschutzaufsichtsbehörden.**
   Die zuständigen Landesdatenschutzbeauftragten sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sollen prüfen, ob der Ankauf und die Nutzung kommerzieller Standortdaten durch Sicherheitsbehörden mit den Vorgaben der DSGVO sowie dem Grundrecht auf informationelle Selbstbestimmung vereinbar sind. Festgestellte Verstöße müssen konsequent beanstandet und beendet werden.

3. **Verbindliche Transparenz- und Berichtspflichten für Sicherheitsbehörden gegenüber den Parlamenten.**
   Parlamente müssen nachvollziehen können, ob und in welchem Umfang Sicherheitsbehörden kommerzielle personenbezogene Datensätze erwerben oder nutzen. Art, Umfang, Rechtsgrundlage und Zweck solcher Datenkäufe sind regelmäßig offenzulegen.

4. **Konsequente Regulierung des Handels mit personenbezogenen Standort- und Bewegungsdaten.**
   Unternehmen, die personenbezogene Standortdaten sammeln, aufbereiten oder weiterverkaufen, müssen einer wirksamen datenschutzrechtlichen Kontrolle unterliegen. Geschäftsmodelle, die auf der massenhaften Vermarktung personenbezogener Bewegungsprofile beruhen, dürfen keinen Platz im europäischen Binnenmarkt haben.

5. **Keine Aufnahme einer Befugnis zum Ankauf oder zur Nutzung kommerziell gehandelter Standortdaten in das neue Thüringer Polizeiaufgabengesetz.**
   Im Zuge der aktuellen Novellierung des Thüringer Polizeiaufgabengesetzes dürfen keine Rechtsgrundlagen geschaffen werden, die den Ankauf oder die Nutzung kommerzieller Standort- und Bewegungsdaten ermöglichen oder erleichtern. Thüringen darf die bestehenden rechtlichen Unsicherheiten nicht durch neue Überwachungsbefugnisse verschärfen.

Antragsbegründung

Erfolgt mündlich.