PRESSEMITTEILUNG

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 02.04.2026

Datenschutzkonferenz: Geplante digitale Ermittlungsbefugnisse gehen zu weit – Grundrechtschutz muss eingehalten werden

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) kritisiert drei Gesetzesinitiativen der Bundesregierung zur Erweiterung digitaler Ermittlungsbefugnisse. Nach den Gesetzesplänen sollen die automatisierte Datenanalyse und der biometrische Abgleich mit Daten aus dem Internet in Strafverfahren sowie für die Polizeibehörden des Bundes zur Gefahrenabwehr eingeführt werden. In der vorgesehenen Form sind diese Befugnisse nicht mit den verfassungsrechtlichen Vorgaben vereinbar. Sie gefährden die verfassungsrechtlich geschützten Rechte Unbeteiligter erheblich. Die DSK fordert die Bundesregierung deshalb auf, gegenüber der Bevölkerung maßvoll vorzugehen und die Grundrechte Unbeteiligter besser zu schützen.

Die Regelung zum biometrischen Online-Abgleich ermöglicht es den Behörden, bei ihnen vorhandene Daten mit sämtlichen im Internet öffentlich zugänglichen Daten abzugleichen, um beispielsweise anhand von Gesichtsbildern oder Stimmproben Personen zu identifizieren. Auch Daten kostenpflichtiger Internetdienste oder solcher, für die ein Benutzerkonto angelegt werden muss, sind von der Entwurfsregelung umfasst. Damit kann nahezu jede und jeder von solchen Maßnahmen betroffen sein. Jedes im Internet veröffentlichte Bild, Video und jede Tonaufnahme können Gegenstand eines solchen Abgleichs werden. Dies führt nicht nur zu einem Gefühl des Überwachtwerdens, sondern kann im Fall von Falscherkennungen konkrete Konsequenzen für die betroffene Person haben. Auch die Bildung von Bewegungs- und Verhaltensprofilen ist nicht ausgeschlossen.

Die geplante Regelung zur automatisierten Datenanalyse soll es den Behörden ermöglichen, die bei ihnen vorhandenen Daten in einer Analyseplattform zusammenzuführen und mit automatisierten Verfahren zu analysieren, um daraus neue Erkenntnisse für die Strafverfolgung oder die Abwehr von Gefahren zu gewinnen. Der Datenbestand der Analyseplattform ist weit gefasst: Er enthält neben den polizeilichen Informationssystemen etwa Daten aus polizeilichen Vorgangsbearbeitungssystemen, aus Funkzellenabfragen, Asservate aus

Strafverfahren, z.B. beschlagnahmte Datenträger, bis zu im Einzelfall aus Internetquellen erhobenen Datensätzen. Auch die für den biometrischen Abgleich erhobenen Internetdaten können in den Abgleich einbezogen werden. Damit beschränkt sich die Analyse nicht auf Personen, die als Tatverdächtige oder Gefährdende bereits auffällig geworden sind. Es können Zeuginnen und Zeugen, Anzeigende, Geschädigte, Kontaktpersonen und auch gänzlich unbeteiligte Personen einbezogen werden. Durch Datenanalysen kann neues Wissen erzeugt werden, z.B. können Zusammenhänge zwischen Personen, Institutionen, Organisationen oder Objekten hergestellt werden. Daraus entsteht für die betroffenen Personen das Risiko, zum Gegenstand von Ermittlungen oder Maßnahmen zu werden.

Durch den Einsatz von Künstlicher Intelligenz erhöhen sich die Risiken für betroffene Personen nochmals. Auch für die Nachvollziehbarkeit und Transparenz der Verfahren und der Ergebnisse für die einsetzenden Behörden selbst, die betroffenen Personen sowie Gerichte und Aufsichtsbehörden stellen sich dadurch besondere Herausforderungen.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg und Vorsitzender der Datenschutzkonferenz 2026 Prof. Dr. Tobias Keber: „Wenn der Gesetzgeber die Notwendigkeit für die Einführung solcher Befugnisse sieht, dann muss er auch klar regeln, dass sie die Ausnahme bleiben und sich die Eingriffe auch im Einzelfall auf das Nötigste beschränken. Wenn potenziell unbescholtene Menschen immer und überall ins Visier der Strafverfolgungsbehörden geraten können und von einem autonomen System gescannt werden können, geht das zu weit. Für alle Eingriffsbefugnisse gilt es, die Vorgaben des Bundesverfassungsgerichts zu beachten. Die unterschiedlichen Gesetzesinitiativen ermöglichen zusammengenommen eine umfassende Überwachung der Menschen. Hier führt der durchaus nachvollziehbare Wille zu mehr Sicherheit zu einem zu starken Eingriff des Staates in die Grundrechte seiner Bürger_innen.“

Die DSK sieht zweifellos, dass es zur Aufklärung von Straftaten und zur Gefahrenabwehr Regelungen geben muss, die den digitalen Bereich einbeziehen. Die DSK unterstützt eine zügige und wirksame Rechtsdurchsetzung im Rahmen der verfassungsrechtlichen Grenzen. Statt der vom Bundesgesetzgeber vorgeschlagenen Vorgehensweise wäre ein Grundrechtsausgleich mit abgestuften und ausdifferenzierteren Befugnissen nötig und auch möglich, wie sie das Bundesverfassungsgericht für die automatisierte Datenanalyse ausführlich beschrieben hat. Stellschrauben wären der Umfang der einzubeziehenden Daten,

die Methoden des Abgleichs und der Analyse (z.B. ein Ausschluss von Künstlicher Intelligenz, wenn sie nicht durchgehend kontrolliert werden kann), die Anlässe und die Voraussetzungen für die Grundrechtseingriffe, z.B. eine enge und klare Definition der Straftaten, zu deren Verfolgung die Maßnahmen ergriffen werden dürfen.

Weitere Informationen:
Derzeit gibt es drei Gesetzesinitiativen auf Bundesebene zu digitalen Ermittlungsmaßnahmen im Bereich der Gefahrenabwehr und Strafverfolgung:

1. Das „Gesetz zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“ vom Bundesministerium der Justiz und für Verbraucherschutz: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/2026_Digitale_Ermittlungsverfahren.html?nn=110490;

2. „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“ vom Bundesministerium des Inneren: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/OESI3/ermittlungsbefugnisse-polizeiarbeit.html;

3. „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“ vom Bundesministerium des Inneren: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/OESI3/ermittlungsbefugnisse-abwehr-int-terrorismus.html

Die Datenschutzkonferenz hat sich in den vergangenen Jahren mehrfach zu Befugnissen von Sicherheitsbehörden geäußert:

Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten: https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Datenanalyse-Polizei.pdf

Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten: https://www.datenschutzkonferenz-online.de/media/en/2025-09-17_DSK-Entschliessung_Automatisierte-Datenanalyse.pdf

Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörde: https://www.datenschutzkonferenz-online.de/media/en/2024-09-20_Entschliessung_DSK_Gesichtserkennung.pdf