Entschließung

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden

des Bundes und der Länder vom 17. September 2025

Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten!

Die aktuelle politische Diskussion über den Einsatz von Verfahren zur automatisierten Datenanalyse durch die Polizei betrifft rechtliche und technische Anforderungen an polizeiliches Handeln, die auch unter dem Gesichtspunkt der digitalen Souveränität betrachtet werden sollten. Die bisher bekannten Analyseverfahren, die die Polizei in einzelnen Ländern für die Gefahrenabwehr einsetzt, können jede und jeden betreffen. Nicht nur Straftäterinnen und Straftäter, sondern etwa auch Geschädigte, Zeuginnen und Zeugen, Sachverständige oder Personen, die den Polizeinotruf genutzt haben, können in eine solche Analyse einbezogen sein: Allein in Bayern bezieht sich das dortige Analyseverfahren auf circa 39 Millionen Personendatensätze. Es ist verfassungsrechtlich selbstverständlich, dass die Polizei nur bei sehr schwerwiegenden Rechtsgutverletzungen und unter ganz engen Verfahrensbestimmungen solche einschneidenden Analysemittel einsetzen darf. Vor diesem Hintergrund fordert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die Einhaltung grundlegender, teils auf der Rechtsprechung des Bundesverfassungsgerichts beruhender, Anforderungen.

1. Kein Einsatz von komplexen Datenanalyseverfahren ohne spezifische Rechtsgrundlage

Die DSK betont, dass die allgemeinen Vorschriften im Polizeirecht und in der Strafprozessordnung den Besonderheiten komplexer Analysemethoden nicht ausreichend Rechnung tragen, die mit intensiven Eingriffen in die Grundrechte der betroffenen Personen verbunden sein können. Dies gilt insbesondere für Analysen von umfassenden Datenbeständen, die – wie eingangs beschrieben – Daten über Personen enthalten, die durch ihr Verhalten keinen Anlass für polizeiliche Ermittlungen gegeben haben. Durch Datenanalysen kann neues Wissen erzeugt werden, zum Beispiel können Zusammenhänge zwischen Personen, Institutionen, Organisationen oder Objekten hergestellt werden. Daraus entsteht für die betroffenen Personen das Risiko, zum Gegenstand polizeilicher Ermittlungen oder Maßnahmen zu werden. Dies greift in die Grundrechte aller hiervon betroffenen Personen ein; für die Personen, die selbst

keinen Anlass hierfür gegeben haben, wiegt dieser Eingriff besonders schwer. Für solche komplexen Analysen bedarf es eigener Rechtsgrundlagen, die nach dem Gewicht der unterschiedlichen Grundrechtseingriffe bei der Erhebung und Weiterverarbeitung der Daten differenzieren müssen. Wird ihr Einsatz fachlich als erforderlich angesehen, ist der Gesetzgeber in der Pflicht, die wesentlichen Grundlagen selbst durch spezifische gesetzliche Vorschriften vorzugeben, um insbesondere Art und Umfang der Daten und die Verarbeitungsmethoden zu begrenzen. Dies umfasst grundlegende Anforderungen an die notwendigen technischen Anwendungen und Infrastrukturen.

2. Die gesetzliche Grundlage muss verfassungsrechtlichen Maßstäben genügen

Das Bundesverfassungsgericht hat sich im Urteil vom 16. Februar 2023 (- 1 BvR 1547/19 - und - 1 BvR 2634/20 -) umfassend mit dem behördlichen Einsatz von automatisierten Datenanalysen befasst und hierfür die verfassungsrechtlichen Weichen gestellt. Das Bundesverfassungsgericht hat entschieden, dass das Gewicht des mit der Datenanalyse verbundenen Grundrechtseingriffs insbesondere durch Art und Umfang der zu verarbeitenden Daten und die zugelassene Methode der Datenanalyse bestimmt wird.

Ein besonderes Eingriffsgewicht aufgrund von Art und Umfang der Daten ist regelmäßig gegeben, wenn viele Daten zu Personen in die Datenanalyse eingehen, die selbst keinen Anlass für polizeiliche Maßnahmen gegeben haben oder wenn die Daten verschiedenster Systeme trotz ursprünglich unterschiedlicher Erhebungs- und Verarbeitungszwecke in eine Gesamtauswertung einbezogen werden (Zweckbindung und Zweckänderung). Das trifft beispielsweise auf Datenbestände aus der Vorgangsbearbeitung und aus Maßnahmen mit großer Streubreite wie Funkzellenabfragen zu. Funkzellenabfragen betreffen alle Personen, die in der Funkzelle mit ihrem Mobilgerät eingebucht sind. Datenbestände insbesondere aus Vorgängen der Strafverfolgung enthalten regelmäßig auch Daten von Geschädigten sowie Zeuginnen und Zeugen. Die herangezogenen Datenbestände müssen für den Zweck der konkreten Datenanalyse geeignet sein. Den Verhältnismäßigkeitsanforderungen genügt eine Maßnahme der Datenverarbeitung grundsätzlich nur, wenn die einzubeziehenden Daten auf solche beschränkt werden, die für den jeweiligen Zweck der Maßnahme Bedeutung haben können.

Besonderes Eingriffsgewicht aufgrund der Methode der Datenanalyse können insbesondere die Verwendung lernfähiger Systeme – Künstliche Intelligenz („KI“) –, aber auch komplexe Formen des Datenabgleichs mit nicht lernfähigen Systemen haben. Die DSK sieht ihre Forderungen aus ihrer Entschließung vom 3. April 2019 „Hambacher Erklärung zur Künstlichen Intelligenz“ in dem Urteil bestätigt.

Ermöglicht das Verfahren nach den vom Bundesverfassungsgericht benannten Kriterien schwerwiegende Grundrechtseingriffe, ist ein Einsatz nur zum Schutz gewichtiger Rechtsgüter – wie etwa Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes – und unter strenger Begrenzung des Anlasses für die Maßnahme zulässig. Außerdem sind Transparenz und individueller Rechtsschutz für die betroffenen Personen und eine aufsichtliche Kontrolle gesetzlich vorzusehen.

3. Die digitale Souveränität muss bei der Auswahl von Verfahren gewährleistet werden

Sollen für die Analysen Systeme von Fremdanbietern eingesetzt werden, kommen nicht nur die gesetzlichen Anforderungen an die Datensicherheit gegenüber dem Anbieter zum Tragen, sondern es ist auch sicherzustellen, dass die digitale Souveränität des Staates gewahrt wird. Ganz besonders bei polizeilichen Datenbeständen hat der Staat gegenüber seinen Bürgerinnen und Bürgern eine Schutzpflicht, dass deren Daten nicht ohne vorherige Prüfung in Drittstaaten weiterverwendet werden können, die hinter dem europäischen Rechtsstaatsniveau zurückbleiben. Die DSK hat zur Gewährleistung der digitalen Souveränität bei Cloud-Lösungen Kriterien erarbeitet, die sinngemäß auch auf Datenanalyseverfahren für die Polizei übertragbar sind (Kriterien für Souveräne Clouds – Positionspapier der DSK vom 11. Mai 2023). Zu diesen Anforderungen gehört der Ausschluss von Zugriffen aus oder Datentransfers in Drittstaaten, deren Rechtsordnung nicht mit dem europäischen Recht vereinbar ist. Darüber hinaus verlangt die digitale Souveränität die Nachvollziehbarkeit und die Beherrschbarkeit der Datenverarbeitung, auch im Wege außergerichtlicher oder gerichtlicher Rechtsdurchsetzung, und die langfristige Vorhersehbarkeit und Verlässlichkeit des Angebots. Diese Ziele können in aller Regel zuverlässig nur durch den Einsatz von Systemen erreicht werden, deren Anbieter ihren Sitz im Europäischen Wirtschaftsraum (EWR) haben.

Zur Wahrung der digitalen Souveränität durch Unterbindung von Abhängigkeiten ist zudem sicherzustellen, dass die eingesetzten Systeme hinreichend offen sind, um nötigenfalls einen Wechsel auf ein geeigneteres System zu ermöglichen.

4. Projekt P20 als Chance für den Datenschutz nutzen

Mit dem IT-Großprojekt „Polizei 20/20“ (P 20) wird bereits seit längerem eine gemeinsame IT-Infrastruktur der Polizeibehörden von Bund und Ländern vorbereitet. In diesem Projekt besteht die Möglichkeit, datenschutzkonforme Auswerte- und Analysetools zu entwickeln, gegebenfalls auf Basis von transparenten und kontrollierbaren Open Source-Produkten. Auf dem Markt angebotene umfassende Analysetools können nach hiesiger Einschätzung nicht ohne erheblichen Aufwand die im Projekt zu realisierenden Anforderungen an einen verfassungsgemäßen Austausch von Daten zwischen Bund und Ländern erfüllen.

Die Datenschutzkonferenz bietet weiterhin ihre konstruktive Beratung an, um im Rahmen des Projekts P20 verfassungskonforme und praxistaugliche Lösungen der Datennutzung für die Polizeien zügig auf den Weg zu bringen. Dies gilt auch in Bezug auf etwaige Analysetools.