Verfassungswidrige Superdatenbank

Die dauerhafte Zusammenführung polizeilicher Datenbestände als eigenständiger Grundrechtseingriff

Jonas Botta

01.09.2026 doi: 10.59704/8b01ca2f7ffd04f8

Die automatisierte Datenanalyse soll Gefahrenabwehr und Strafverfolgung effizienter machen. Über ihre Verfassungsmäßigkeit wird gestritten[1] – bislang aber fast nur über die konkrete Analyse und ihre materiellen Voraussetzungen. Kaum Beachtung findet, dass schon deren technische Vorbereitung schwerwiegend in Grundrechte eingreift: Die zuständigen Polizeibehörden können die zu durchsuchenden Datenbestände nicht nur anlassbezogen für den einzelnen Suchvorgang verknüpfen, sondern sie zu einem dauerhaften Informationspool zusammenführen – inklusive der Daten von Geschädigten, Zeugen und Unbeteiligten. Eine derartige Superdatenbank stellt einen eigenständigen Grundrechtseingriff dar. Weil die (geplanten) Ermächtigungsgrundlagen in Bund und Ländern weder Speicherschwellen noch Speicherdauern für die betroffenen Daten vorsehen, sind sie schon in dieser Hinsicht verfassungswidrig.

Speicherung eines Grunddatenbestandes unabhängig vom Einzelfall und Eingriffsschwellen

In den vergangenen Jahren haben zahlreiche Landesgesetzgeber ihre Polizeigesetze umfassend modernisiert. Zu den neuen digitalen Befugnissen zählt insbesondere die automatisierte Datenanalyse.[2] Sie soll vorhandene Datenbestände nicht nur besser durchsuchbar machen, sondern aus ihnen neues Wissen gewinnen. Auch der Bund will nachziehen und plant entsprechende Regelungen im BKAG, im BPolG und in der StPO.[3]

Trotz unterschiedlichem Wortlaut ist diesen Vorschriften gemein, dass sie einen gestuften Verarbeitungsprozess vorsehen. Zunächst sind die Daten zusammenzuführen, dann zu analysieren. So statuiert beispielsweise § 9b Abs. 1 S. 1 BKAG-E: „Das Bundeskriminalamt kann zur Erfüllung der Aufgabe als Zentralstelle Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, nach Maßgabe von § 12 mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten […]“.[4]

Für welche Dauer die zuständigen Polizeibehörden ihre Datenbestände zusammenführen dürfen, ergibt sich aus den (vorgeschlagenen) Rechtsgrundlagen auf Bundes- und Landesebene nicht eindeutig. Rein nach dem Wortlaut wäre denkbar, dass die Zusammenführung stets unmittelbar der Analyse vorausgeht und deshalb nur einen temporären Datenpool bildet. Tatsächlich soll jedoch eine dauerhafte Zusammenführung zumindest eines Grunddatenbestandes erfolgen – welche Daten dazu zählen, bleibt offen.

In der Gesetzesbegründung des § 9b BKAG-E heißt es dazu, eine Zusammenführung nur im Einzelfall werde dem Zweck schneller und effektiver Straftatenverhütung und -verfolgung wegen der Masse der Daten nicht gerecht; sie müsse deshalb „vom Einzelfall und weiteren Eingriffsschwellen unabhängig sein“.[5] Ähnlich argumentieren die Gesetzesmaterialien auf Landesebene: Ein für die Analyse aufbereiteter Daten-

[1] Weiterführend z.B. Michael Bäuerle, in: *Möstl/Bäuerle, BeckOK PolR Hessen* (38. Aufl., 2026), § 25a HSOG Rn. 37 ff.
[2] Ein Überblick über die Rechtslage in den Ländern findet sich beispielsweise bei Mario Martini und Jonas Botta, *Polizeiliche Datenanalyse mittels KI: Unions-, verfassungs- und polizeirechtliche Leitplanken für Palantir & Co*, DÖV (2025), S. 1033 (1039 ff.).
[3] BT-Drs. 21/6132 und BT-Drs. 21/6806.
[4] BT-Drs. 21/6132, S. 9.
[5] S. Fn. 4, S. 28.

bestand müsse unmittelbar bereitstehen.[6] Der Grunddatenbestand soll also entstehen, bevor überhaupt der Anlass für eine Analyse gegeben ist.

Gleichwohl regeln die Gesetzgeber in Bund und Ländern diese Superdatenbank nicht näher. Die Gründe dafür lassen sich der Begründung zu § 23 Abs. 6 PolG NRW entnehmen: Die automatisierte Zusammenführung sei keine rechtfertigungsbedürftige Datennutzung, sondern nur deren technische Voraussetzung.[7] Diese Sichtweise überzeugt jedoch nicht.[8]

Eingriffsqualität der dauerhaften Datenzusammenführung

Bereits die dauerhafte Datenzusammenführung greift in das Recht auf informationelle Selbstbestimmung ein. Denn die Erhebung, Speicherung und Verwendung personenbezogener Daten sind jeweils unterschiedliche Grundrechtseingriffe.[9] Bei der Datenzusammenführung handelt es sich um einen eigenständigen Speichervorgang – obwohl die Informationen bereits in den polizeilichen Systemen vorliegen. Maßgeblich ist, dass die Zusammenführung einen neuen, eigenständigen Datenbestand schafft, in dem die Informationen über Datei-, Format- und Systemgrenzen hinweg wechselseitig verknüpfbar sind. Genau diese Verknüpfbarkeit erzeugt ein spezifisches grundrechtliches Risiko.[10] Ein über mehrere Systeme verteilter Bestand erlaubt keine übergreifenden Persönlichkeitsprofile; eine Superdatenbank tut es. Daher steht der Eingriffsqualität auch nicht entgegen, dass es zum Zeitpunkt der Datenzusammenführung offen ist, ob die einzelnen Informationen später tatsächlich in einem Suchvorgang Berücksichtigung finden. Denn das Recht auf informationelle Selbstbestimmung schützt bereits im Vorfeld konkreter Bedrohungen.[11]

Eingriffsintensität der dauerhaften Datenzusammenführung

Das Gewicht eines Eingriffs in die informationelle Selbstbestimmung richtet sich vor allem nach Art, Umfang und denkbarer Verwendung der Daten sowie der Gefahr ihres Missbrauchs.[12] Daran gemessen weist die polizeiliche Superdatenbank eine besondere Eingriffsintensität auf. Zwar schweigen Gesetzeswortlaut wie Gesetzesbegründung der einschlägigen Vorschriften dazu, welche Datenkategorien zum dauerhaft gespeicherten Grunddatenbestand zählen sollen. Sie geben aber vor, welche Informationen in die nachfolgende Analyse einfließen dürfen. Daraus lässt sich ablesen, welcher Umfang dem Grunddatenbestand zukommen könnte – selbst wenn er seiner Bezeichnung entsprechend tatsächlich nur einen Ausschnitt der analysefähigen Daten erfassen sollte.

Auf der Analyseplattform lassen sich zahlreiche Informationen zusammenführen: Vorgangsdaten, Falldaten, Daten aus dem Informationssystem der Polizei, zum Abruf durch die Polizei im polizeilichen Informationssystem zwischen Bund und den Ländern bereitstehende Daten (INPOL-neu), Daten aus dem polizeilichen Informationsaustausch, Verkehrsdaten aus Funkzellenabfragen, Telekommunikationsdaten und Daten aus Asservaten. Besonders die Vorgangsdaten dürften zu einer hohen Informationsdichte führen, denn ein Vorgang umfasst alles, was die Polizei zu einer Person oder Sache anlegt: Anzeigen, Ermittlungsberichte, Vermerke usw. Eingang in die Analyseplattform finden damit gerade auch die personenbezogenen Daten von Menschen, die keine polizeirechtlichen Störer oder (mutmaßlichen) Straftäter sind – Geschädigte, Zeugen und Unbeteiligte (vgl. § 9b Abs. 2 Nr. 2 BKAG-E). Auf diesen fehlenden Anlass kommt es für das Eingriffsgewicht maßgeblich an.[13] Hinzu kommen externe Datenbestände, auf die die Polizei zugreifen kann, etwa das

[6] Siehe z.B. LSA-LT-Drs. 8/5018, S. 58.
[7] NRW-LT-Drs. 17/16517, S. 17: „Dieser [der Zweckbindungsgrundsatz] wird jedoch bei der automatisierten Zusammenführung der Daten voll eingehalten, da die automatisierte Zusammenführung als solche noch keine Nutzung der Daten für die polizeiliche Aufgabenerfüllung beinhaltet, sondern nur eine technische Voraussetzung für diese Nutzung darstellt."
[8] Ebenso Clemens Arzt, in: *Möstl/Kugelmann, BeckOK PolR NRW* (34. Aufl., 2026), § 23 PolG NRW Rn. 56 ff.
[9] Vgl. BVerfG, 1 BvR 142/15, 18.12.2018, Rn. 42.
[10] Vgl. Fn. 9, Rn. 37.

Melde- und Waffenregister. Zwar ist eine direkte Anbindung an das Internet unzulässig, doch dürfen einzeln gespeicherte Daten aus allgemein zugänglichen Quellen wie sozialen Medien ergänzend zusammengeführt werden (vgl. § 9b Abs. 3 S. 2 BKAG-E). Sogar von Nachrichtendiensten übermittelte Daten können in die Analyseplattform einbezogen werden.

Zukünftig dürfte der analysefähige Datenbestand zudem noch deutlich anwachsen. Denn Bund und Länder wollen im Rahmen des Programms „P20“[14] ein gemeinsames „Datenhaus“ errichten, in dem alle polizeilich verfügbaren Informationen in grundsätzlich getrennten, aber verknüpfbaren Bereichen zusammenfließen sollen.[15] Dieses „Datenhaus“ kann dann die technische Grundlage für die automatisierte Datenanalyse aller deutschen Polizeibehörden bilden.

Zusätzlich erhöht die Heimlichkeit der Datenzusammenführung das Eingriffsgewicht, da sie den nachträglichen Rechtsschutz der Betroffenen erheblich einschränkt.[16]

Rechtfertigungsanforderungen an die dauerhafte Datenzusammenführung

Als eigenständiger Grundrechtseingriff bedarf die dauerhafte Datenzusammenführung einer spezifischen Rechtfertigung.[17] Die dafür maßgeblichen Vorgaben folgen aus der Rechtsprechung des BVerfG. Zwar hat Karlsruhe in seinem „hessenDATA“-Urteil aus dem Jahr 2023 zu einer anlasslosen Speicherung der Analysegrundlagen geschwiegen, da das Gericht wohl davon ausgegangen ist, dass die Polizei die betroffenen Daten nur für den konkreten Suchvorgang zusammenführt.[18] Aber im Folgejahr setzte sich das BVerfG in seinem „BKAG II“-Urteil umfassend mit der vorsorgenden Speicherung von Daten im polizeilichen Informationsverbund auseinander.[19] Um einen derartigen Verarbeitungsvorgang handelt es sich auch bei der polizeilichen Superdatenbank: Daten werden auf Vorrat in einem neuen Zusammenhang bereitgehalten, entkoppelt vom ursprünglichen Erhebungszweck und von der konkreten späteren Analyse.[20]

Verfassungsrechtlich lässt sich die vorsorgende Speicherung nur unter drei Bedingungen rechtfertigen. Erstens muss der Gesetzgeber einen konkreten Speicherzweck festlegen.[21] Insbesondere ist es der Polizei versagt, alle rechtmäßig erhobenen Informationen allein mit der Begründung vorrätig zu halten, man könne sie später vielleicht noch weiterverarbeiten. Ein Vorrat, dessen Zwecksetzung derart offen bliebe, ließe den Grundsatz der Zweckbindung gänzlich leerlaufen.[22] Zweitens bedarf es einer Speicherschwelle, die den Zusammenhang zwischen den vorrätig gehaltenen Daten und dem Speicherzweck garantiert.[23] Bei der Verhütung und Verfolgung von Straftaten ist das nur erfüllt, wenn eine hinreichende Wahrscheinlichkeit besteht, dass die Betroffenen eine strafrechtlich relevante Verbindung zu möglichen Straftaten aufweisen und gerade die gespeicherten Daten zur Verhütung und Verfolgung beitragen können. Diese Prognose muss sich auf zureichende tatsächliche Anhaltspunkte stützen. Drittens braucht es eine angemessene, differenzierte und zeitlich begrenzte Speicherdauer, weil eine Prognose über die Zeit an Überzeugungskraft verliert, wenn nicht neue, relevante Umstände hinzutreten.[24]

Gemessen an diesem Maßstab erweisen sich die Befugnisnormen zur dauerhaften Datenzusammenführung als unverhältnismäßig. Selbst wenn man in der Ermöglichung der automatisierten Datenanalyse einen tauglichen Speicherzweck sieht, koppeln der Regierungsentwurf des § 9b BKAG-E und seine landesrechtlichen Pendants die Speicherung doch bewusst vom Einzelfall und von jeder Eingriffsschwelle ab. Auch sehen die Rechtsgrundlagen keine ausreichenden Speicherfristen für den Grunddatenbestand vor.[25] Diese Leerstellen lassen sich nicht auf der Vollzugsebene

[11] S. Fn. 9, Rn. 37.
[12] BVerfG, 1 BvR 1160/19, 1.10.2024, Rn. 157.
[13] Vgl. Fn. 12.
[14] Auch „Polizei 20/20“ genannt.
[15] Bundesministerium des Innern und für Heimat, *P20 – Auf dem Weg zu einer gemeinsamen, digitalen und vernetzten Polizei*, 05.06.2023, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI23004.pdf?__blob=publicationFile&v=7, zuletzt abgerufen am 22.07.2026.

ausfüllen. Speicherschwelle und Speicherdauer betreffen das Ob und das Wie der vorsorgenden Speicherung – also Fragen, die der Gesetzgeber selbst entscheiden muss und nicht der Exekutive überlassen darf.

Von der Datenbank zu Palantirs Ontologie

Hinzu tritt ein weiterer Malus: Den Rechtsgrundlagen fehlen Schutzmechanismen für den Fall, dass die dauerhafte Datenzusammenführung mittels proprietärer Software erfolgt, was insbesondere das Risiko unbemerkter Manipulation und unberechtigter Zugriffe birgt.[26] Derzeit setzt die Polizei zur automatisierten Datenanalyse allein auf die Software „Gotham“ von Palantir. Das US-amerikanische Unternehmen liefert dabei nicht bloß eine Datenbankinfrastruktur, sondern eine eigene Ontologie – ein Ordnungsmodell dafür, wie Daten definiert, strukturiert und zueinander in Beziehung gesetzt werden.[27] Damit gibt der Staat die Hoheit über seine Informationsbestände aus der Hand und droht gerade die technologische Souveränität zu verlieren, die digitale Polizeiarbeit im demokratischen Rechtsstaat voraussetzt.

Polizeiliches Datenhaus ohne tragendes Fundament

Die dauerhafte Zusammenführung personenbezogener Daten zu einer polizeilichen Superdatenbank ist ein eigenständiger und schwerwiegender Grundrechtseingriff. Die (vorgeschlagenen) Rechtsgrundlagen auf Bundes- und Landesebene verfehlen die bundesverfassungsgerichtlichen Anforderungen an diese vorsorgende Speicherung und sind daher verfassungswidrig.

Dieser Befund hat Konsequenzen für die ganze Debatte über die automatisierte Datenanalyse. Wer allein über die konkrete Analysemöglichkeit streitet – über Suchanfragen, Eingriffsschwellen, menschliche Letztentscheidung –, diskutiert über das zweite Stockwerk eines Gebäudes, dessen Fundament nicht trägt. Das geplante „Datenhaus“ der Polizeibehörden des Bundes und der Länder ist schon vor seinem Richtfest einsturzgefährdet.

AUTOR*IN
Jonas Botta
Jonas Botta ist Juniorprofessor für Öffentliches Recht mit einem Schwerpunkt im Recht der Digitalisierung und der Künstlichen Intelligenz an der FernUniversität in Hagen.

EMPFOHLENE ZITATION
Botta, Jonas: Verfassungswidrige Superdatenbank: Die dauerhafte Zusammenführung polizeilicher Datenbestände als eigenständiger Grundrechtseingriff, Verfassungsblog, 01.09.2026, doi: 10.59704/8b01ca2f7ffd04f8.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260902-150453-0.

[16] Vgl. Fn. 12, Rn. 170.
[17] Vgl. Fn. 12, Rn. 90.
[18] Vgl. BVerfG, 1 BvR 1547/19, 1 BvR 2634/20, 16.02.2023; Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drs. 20/12806, Ausschuss-Drs. 20(4)483, S. 8.
[19] S. Fn. 12; dazu z.B. Sebastian J. Golla, *Aufräumen im Datenhaus: Die polizeiliche Datenspeicherung nach BVerfG, BKAG II*, Verfassungsblog, 01.10.2024, DOI: 10.59704/9f09752ec0067580, zuletzt abgerufen am 22.07.2026.
[20] Vgl. Fn. 12, Rn. 158.

[21] S. Fn. 12, Rn. 182.

[22] S. Fn. 12, Rn. 183.

[23] Fn. 12, Rn. 184.

[24] S. Fn. 12, Rn. 184.

[25] Vgl. Clemens Arzt, in: *Möstl/Kugelmann, BeckOK PolR NRW* (34. Aufl., 2026), § 23 PolG NRW Rn. 67 f.

[26] Vgl. BVerfG Fn. 18, Rn. 100.

[27] Weiterführend zu Palantirs Ontologie etwa Imke Stock, *Missing Link: Machtzentrale Palantir – eine Software lenkt Organisationen*, heise online, 29.06.2025, https://heise.de/-10463034, zuletzt abgerufen am 22.07.2026; vgl. Elena Esposito und Simon Egbert, Palantir und digitale Souveränität, Verfassungsblog, 26.08.2026, DOI: 10.59704/70233c5f9182b075, zuletzt abgerufen am 1.09.2026.